Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas y Telemática

Directrices para la construcción de un software y administración del proyecto de un SGSI, basado en la metodología ECU@Risk.

Tesis de grado previo a la obtención del título de Ingeniero de Sistemas y Telemática

Autor: Pablo Andrés Cevallos Ordóñez.

Director: Ing. Esteban Crespo.

Cuenca, Ecuador

2018

DEDICATORIA

El presente trabajo va dedicado a todas las personas que estuvieron a mi lado a lo largo de mi formación profesional y en el desarrollo de este trabajo de titulación. A mi enamorada, por el constante apoyo, paciencia y ánimos que me ha brindado, a mis padres por los consejos y dedicación, a mi hermana por el ejemplo e inspiración que ha sembrado en mí para salir adelante a pesar de las adversidades. A todas estas personas quiero dedicarles mi esfuerzo que he puesto en la realización de este trabajo.

AGRADECIMIENTOS

Agradezco a primero a Dios por darme la vida y salud, a mis familiares y amigos que estuvieron a mi lado en momentos duros de mi vida, gracias a todos por bridarme su cariño y su apoyo. Quiero agradecer a todos los profesores que han sido parte de mi formación académica, en especial a mi querido profesor Esteban Crespo, quien con mucho esmero supo guiarme en la elaboración de este proyecto.

ÍNDICE DE CONTENIDOS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

RESUMEN

En este trabajo se propone el procedimiento y consideraciones para la construcción de un software que facilite la gestión de riesgos de información, basado en la metodología para gestión de riesgos Ecu@Risk aplicable a las MPYMES, considerando los fundamentos en los que se basa en la ingeniería de software: el levantamiento de requerimientos, el diseño del software, la gestión del proyecto de desarrollo, la planificación, el presupuesto y para finalizar la gestión de riesgos del proyecto.

ABSTRACT

In this paper, the procedures and considerations for the development of a software that could facilitate the management of information risks were proposed. The study was based on the Ecu@Risk methodology for risk management, which is applicable to MPYMES. For the development of the software engineering, the following fundamentals were considered: requirement survey, software design, management of the development project, planning, budget and project risk management.

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by

Ing. Paul Arpi

INTRODUCCIÓN:

Las tecnologías de información, servicios y modelos de comunicación e información, y el incremental uso globalizado de Internet, ha incrementado el número de ataques a los sistemas informáticos de las empresas y organizaciones, tratando de comprometer la información que, para una organización, es considerada como un recurso vital. Los crecientes ataques a los sistemas de información han llevado a las empresas a buscar estrategias que permitan analizar herramientas y contramedidas que ayuden prevenir, controlar, reducir, mitigar, transferir o aceptar riesgos que se asocian a la violación o vulneración de la información. (Abril, Pulido, & Bohada, 2013)

Un estudio realizado por Esteban Crespo (2016), da como resultado que en el entorno ecuatoriano la micros, pequeñas y medianas empresas (MPYMES) no son conscientes de la importancia de la seguridad de la información, o no cuentan con los recursos necesarios; por lo tanto, no tienen estrategias o no aplican una metodología para la gestión de riesgos de información.

Crespo (2016) desarrolla una metodología para la gestión de riesgos de información que se adapta al entorno ecuatoriano y que puede ser aplicada a las MPYMES, llamada Ecu@Risk. Esta metodología requiere de un software para que los activos de información y las amenazas latentes que forman parte de sus procesos, procedimientos y actividades sean registradas, evaluadas y controladas correctamente en un entorno informático. Para el desarrollo de este software se emplearon técnicas y buenas prácticas de la ingeniería de software. Además, para desarrollar un producto, se requiere de una correcta identificación y aplicación de una metodología que permita gestionarlo, por cuanto ha sido importante considerar fundamentos de la gestión de proyectos. Este trabajo está dividido en 8 capítulos, clasificados según lo detallado a continuación.

El capítulo 1, estudia los conceptos sobre gestión de riesgos, los conceptos de la ingeniería de software que se aplican en la elaboración de un programa informático y las metodologías existentes para la gestión de un proyecto.

El capítulo 2 analiza la metodología de gestión de riesgos Ecu@Risk, identificando los procesos de la metodología, sus actividades y procedimientos, con el propósito de identificar la información que registra y almacena.

El capítulo 3 se divide en 2 secciones: i) la comparación y posterior análisis de diferentes programas para la gestión de riesgos de información que están disponibles en el mercado actual, mediante una guía de evaluación de software basada en la ISO/IEC 9126; ii) el levantamiento de requerimientos del software en base a la metodología Ecu@Risk.

En el capítulo 4 se indican los aspectos de diseño del software a partir de los requerimientos levantados; el objetivo de la etapa del diseño es sentar las bases sobre las cuales se construirá el software, es decir, es la base sobre la cual se codificará y posteriormente implementará el programa desarrollado. El diseño obedece a los conceptos de ingeniería de software estudiados anteriormente.

La gestión de proyectos es muy importante, ya que da una idea clara de cómo se desarrollará el proyecto, cuánto durará, qué tareas se realizará, cuánto costará, cómo se superará adversidades, etc. Es por eso que en los capítulos: 5, 6 y 7 se abarcarán los temas: gestión del proyecto para la elaboración del software Ecu@Risk, el presupuesto de desarrollo y la gestión de riesgos de elaboración del proyecto, respectivamente.

Finalmente, en el capítulo 8 se presenta la documentación de un prototipo funcional del software Ecu@Risk, desarrollado a partir del levantamiento de requerimientos y diseño elaborados en capítulos anteriores.

Objetivo General:

Proponer directrices para la construcción de un software que permita gestionar los riesgos de información considerando la teoría de la ingeniería de software y la metodología ECU@Risk.

Objetivos Específicos:

1. Fundamentar teóricamente los componentes que permiten el análisis y desarrollo de software bajo principios de ingeniería y buenas prácticas de aseguramiento y calidad.
2. Proponer directrices para levantamiento de requisitos, y el modelamiento del software.
3. Proponer directrices para la gestión del proyecto, contemplando los riesgos que pueden presentarse durante el desarrollo del software para gestión de riesgos de información.

Metodología:

Se aplicarán los conocimientos adquiridos durante los años de estudio de la carrera relacionados con Ingeniería de software y seguridad de la información, específicamente los relacionados con la gestión de riesgos de la información.

Se estudiará e identificará los fundamentos teóricos de la metodología Ecu@Risk con el fin de proponer los lineamientos para la construcción de un software, apoyándose en diferentes fuentes bibliográficas: eventos relacionados con la temática, revistas, conferencias y repositorios de universidades.

La mayor parte del trabajo se centra en el levantamiento de requisitos o análisis de cada uno de los procesos descritos en Ecu@risk, los mismos que serán modelados utilizando las buenas prácticas de la ingeniería de software, considerando aspectos de calidad, gestión de riesgos y gestión de proyectos.

CAPÍTULO 1: Marco teórico

1.1. Introducción

La información es muy importante dentro de una organización, debido a que a lo largo del tiempo ha pasado de ser un "producto" que obtiene la organización por su trabajo, a ser un recurso vital que ayuda a cumplir sus metas y objetivos.

Los autores Abril, Bohada y Pulido (2013) señalan que el desarrollo de Tecnologías de información, servicios y modelos de comunicación e información, y el incremental uso globalizado de Internet, ha llevado a que se aumenten los ataques a los sistemas informáticos de las empresas y organizaciones, tratando de comprometer su información, misma que debe responder siempre a los principios de la seguridad de la información: integridad, disponibilidad y confidencialidad. (Crespo, 2016)

Los crecientes ataques a los sistemas de información han llevado a las empresas a buscar estrategias que permitan analizar herramientas y contramedidas para controlar los riesgos que se asocian a la violación o vulneración de la información. (Abril, Pulido, & Bohada, 2013)

La gestión de riesgos de información es manejada por las empresas para identificar sus activos de información y protegerlos de riesgos que se puedan suscitar. ¿Qué son los riesgos?, la definición que da Sullivan (2016) es "la posibilidad de sufrir daños o pérdidas", es decir, algún evento ocurra y cause daños o pérdidas a la empresa a través de la afectación de los activos de información.

Conocida la definición de riesgo, el autor Sullivan (2016), sugiere tener en consideración cuáles son los componentes del riesgo de seguridad de la información:

- amenazas: factor humano o no humano que hace que explote una vulnerabilidad.
- vulnerabilidad: es lo que explota el actor de amenaza.
- resultados: el resultado de que una vulnerabilidad explote.
- impacto: las consecuencias de los resultados no deseados.

La vulnerabilidad es el componente más crítico para un activo de información; se pueden tomar algunas medidas para controlar la misma, como eliminar por completo una vulnerabilidad, dado que si no existe no puede explotar; si la vulnerabilidad no puede ser eliminada por completo se debe tratar de reducir la probabilidad de que explote, reducir la

impacto que resulte de la explotación de la vulnerabilidad o no realizar ninguna acción y aceptar el riesgo. (Sullivan, 2016)

Establecidos los componentes de riesgo de seguridad de la información, la gestión de riesgos de información según el autor Sullivan (2016) "es el proceso de identificar, comprender, evaluar y mitigar los riesgos y vulnerabilidades subyacentes y el impacto en la información, los sistemas de información y las organizaciones que dependen de la información para sus funciones"; la gestión de riesgos de información dentro de una organización se presenta como las actividades coordinadas que se toman para dirigir y controlar un riesgo. (Crespo, 2016)

Para Sullivan (2016) la gestión de riesgos de información comprende cuatro actividades iterativas: i) identificación de activos de información y riesgos a los que están expuestos, ii) análisis de los riesgos identificados, iii) identificación e implementación de contramedidas que reduzcan o eliminen los riesgos y iv) seguimiento, medición y mejora de las contramedidas implantadas.

En un estudio realizado por Crespo (2016), se puede ver que en el entorno ecuatoriano la micro, pequeña y mediana empresa (MPYME) no tiene una estrategia o metodología para la gestión de riesgos de información que considere la realidad nacional. Algunas Instituciones de control tratan de implementar prácticas internacionales, pero fracasan debido a la cantidad de exigencias de parámetros y procedimientos que las norman requieren.

1.2. Metodología Ecu@Risk

Crespo (2016) desarrolla una metodología para la gestión de riesgos de información que se adapta al entorno ecuatoriano y que puede ser aplicada a las MPYMES, llamada Ecu@Risk, esta metodología proporciona directrices para:

- Identificar el contexto organizacional.
- Registrar los activos de información.
- Identificar y valorar los riesgos y amenazas físicas, de entorno, y lógicas.
- Directrices para el desarrollo de contramedidas y políticas de seguridad.

Ecu@Risk tiene como fundamentos teóricos otras metodologías como: Magerit V3, Microsoft Risk Management, Octave-S y CRAMM. Ecu@Risk está alineada a marcos de gestión como COBIT 5 y COSO III y a las normas internacionales ISO 27001, ISO 27002, ISO 27003 e ISO 27005. (Crespo, 2016)

1.2.1. Procesos de gestión de la metodología Ecu@Risk

La metodología Ecu@Risk se resume en cinco procesos de gestión, un proceso de monitoreo y control y un proceso comunicacional. En la siguiente tabla se presentará el proceso de gestión de riesgo que debe seguir una organización, empresa o institución en el aseguramiento de la información.

Tabla 1:
Resumen de la gestión de riesgos de información según metodología Ecu@Risk.

Paso 1	Determinación de contexto	-Identificar el entorno en que se desenvuelve la empresa. -Identificar el tipo de organización y el tamaño. -Realizar análisis organizacional.
Paso 2	Identificar los activos de información	Tipos de activos -Edificaciones. -Hardware. -Software. -Información electrónica. -Información en papel. -Medios de almacenamiento extraíble. -Infraestructura de comunicaciones. -Recursos humanos.
Paso 3	Identificar riesgos y amenazas	Identificar riesgos - ¿Qué puede pasar? - ¿Cómo puede pasar? - ¿Dónde puede suceder? - ¿Por qué podría suceder? - ¿Cuál podría ser el impacto?
		Identificar amenazas -Activos afectados. -Dimensiones de seguridad afectadas por la amenaza. Tipos de amenaza -Naturales. -Provocados (Intencionales). -Provocados (Por error). -Informáticos. -Comunicaciones.
Paso 4	Análisis de los riesgos	-Identificar controles existentes. -Evaluar probabilidad de que ocurra el riesgo. -Evaluar la consecuencia de la materialización del riesgo. -Valorar el nivel de riesgo.
Paso 5	Evaluación de los riesgos	-Decidir sobre riesgos aceptables y no aceptables, planear acciones futuras. Acciones -No emprender o continuar con el evento, actividad, proyecto o iniciativa. -Tratar activamente el riesgo. -Priorizar las acciones necesarias, si el riesgo es complejo y

		se requiere un tratamiento. -Aceptar el riesgo.
Paso 6	Tratamiento de los riesgos	-Decidir si es necesario un tratamiento específico o si el riesgo puede ser tratado adecuadamente durante el curso de procedimientos normalizados de gestión y actividades de tratamiento específico. -Trabajar en lo que se quiere como deseable para el tratamiento de riesgo. -Identificar y diseñar una opción preferente de tratamiento, una vez que el objetivo del tratamiento ha sido conocido. Evaluar las opciones de tratamiento y su viabilidad en relación con la tolerancia al riesgo. -Documentar el plan de tratamiento de riesgo. -Aplicar tratamientos acordados. -Evaluar el nivel de riesgo residual.
Paso 7	Identificación de contramedidas	Tipo de protección -Protección de tipo general. -Protección de información electrónica y de papel. -Protección de software. -Protección de hardware. -Protección de la infraestructura de comunicaciones. -Seguridad física relativa a edificaciones e instalaciones. -Relativa a los recursos humanos.
Paso 8	Monitoreo y revisión	-Monitoreo continuo. -Reportar de manera formal. -Documentación del riesgo.
Paso 9	Comunicar y consultar	Métodos de comunicación y consulta -Reuniones. -Reportes. -Sistemas en línea. -Talleres de inducción y capacitación de los empleados. -Noticias. -Grupos focales.
		Objetivos del equipo de comunicación -Ayudar a establecer el contexto de forma apropiada -Asegurar los intereses de todos los interesados sean conocidos y considerados. -Asegurar que los riesgos son adecuadamente identificados -Brindar ideas en común sobre áreas de experiencia cuando se asegure o analice el riesgo -Colaborar con la asignación y soporte del plan de tratamiento de riesgos -Comunicar las mejoras logradas en los procesos asociados con el riesgo.

Fuente: (Crespo, 2016)

1.3. Ingeniería de software aplicado a la metodología Ecu@Risk

La metodología Ecu@Risk requiere de un software para que sus procesos, procedimientos y actividades sean registradas, evaluadas y controladas correctamente. Para el desarrollo de este, se requiere el empleo de las técnicas que sugiere la Ingeniería de software, mismas que

deben estar bien fundamentadas, ya sea teóricamente o empíricamente. El objetivo de la Ingeniería de Software no es solo desarrollar un software que "funcione" sino obtener un software de calidad que sea eficiente, libre de errores, etc. Esto se consigue aplicando buenas prácticas y técnicas en todas las fases del desarrollo del software (análisis, diseño, programación, pruebas y mantenimiento). (Cabot Segarra, 2013)

1.4. Ingeniería Web

El objetivo es que el software de la metodología Ecu@Risk esté en la Web, por lo tanto, se debe manejar conceptos de la Ingeniería Web. Se define como a la Ingeniería Web como una especialización de la Ingeniería de Software para el desarrollo de un software que utilice tecnologías web. Las técnicas utilizadas para el desarrollo web toman las mismas técnicas establecidas para la Ingeniería de software, existen otras técnicas que deben ser incluidas como la navegación web concepto muy importante al momento de desarrollar una aplicación web. (Cabot Segarra, 2013)

El primer paso para la construcción de la aplicación es la identificación o levantamiento de requisitos, elementos que ayudan a entender el problema, delimitar el alcance de la propuesta, entre otros aspectos. (Montoya, Pulgarín, & Monsalve, 2014)

1.4.1. Requisitos de análisis para las aplicaciones web

El análisis abarca tres grandes tareas, como indica García Chi (2013):

- Formulación: se identifica las metas y objetivos para la aplicación web.
- Recopilación de requisitos: Se listan los requisitos de contenido y funcionales; desarrollando escenarios de iteración (casos de uso). La iteración es el resolver el por qué se construirá la aplicación, quién la usará y qué problemas resolverá.
- Modelado de análisis: luego de la formulación y recopilación de requisitos, se procede con el modelado de contenido, interacción, funcional, configuración y navegación.

1.4.2. Especificación de requisitos

La especificación de requisitos según el estándar IEEE 830 (ERS), da las pautas para la formulación y levantamiento de los requisitos del software que se encuentre en planes de desarrollar, mediante el establecimiento de objetivos, perspectivas del producto, descripción del producto, identificación de actores, descripción de atributos funcionales y no funcionales

del sistema, etc. Es decir, una descripción completa acerca de la aplicación que se va a desarrollar.

La ERS utiliza los diagramas de Caso de Uso, para identificar a los usuarios que interactuarán con el sistema, facilitando la identificación de los procesos que realiza el software. Son utilizados para mostrar el alcance del software, conjuntamente con las principales características del mismo. (Kendal, 2011)

Las pautas para la especificación de requisitos de software se los resume en la siguiente tabla basado en la norma IEE 830 (IEEE, 2008):

Tabla 2:
Aplicación de la norma IEE 830.

Introducción	Propósito	Se define el propósito del documente ERS, y se especifica a quién va dirigido el documento
	Ámbito del Sistema	-Nombre del futuro sistema. -Se explica lo que el sistema hará y no hará. -Se describe beneficios, objetivos y metas que se espera alcanzar con el futuro software. -Se referencian todos los documentos de nivel superior.
	Definiciones, Acrónimos y Abreviaturas	Se definen todos los términos, acrónimos y abreviaturas utilizadas para el ERS
	Referencias	Lista de todos los documentos referenciados en el ERS.
	Visión General del Documento	Se describe brevemente los contenidos y la organización del resto de la ERS.
Descripción General	Perspectiva del producto	Se relaciona al futuro software con otros productos, si es independiente también se lo indica.
	Funciones del producto	Resumen a grandes rasgos de las funciones del futuro software.
	Características de los usuarios	Se describe las características generales de los usuarios del producto, incluyendo nivel educacional, experiencia y experiencia técnica.
	Restricciones	Se describe las limitaciones que se imponen sobre los desarrolladores del producto.
	Suposiciones y dependencias	Se describen aquellos factores que, si cambian, pueden afectar a los requisitos.
	Requisitos futuros	Se incluyen mejorar al sistema, que podrán analizarse e implementarse en un futuro.
Requisitos específicos	Interfaces externas	Se describe los requisitos que afecten a la interfaz de usuario, interfaz con otros usuarios e interfaces de comunicaciones
	Funciones	Se describe todas las funciones que realizará el software, se lo puede hacer utilizando casos de uso.

	Requisitos de rendimiento	Se detallan los requisitos relacionados con la carga que se espera que tenga que soportar un sistema.
	Restricciones de diseño	Todo lo que restrinja las decisiones relacionadas al diseño de la aplicación.
	Atributos del sistema	Atributos no funcionales del sistema.
	Otros requisitos	Cualquier otro requisito que no encaje en ninguna otra sección.
Apéndices		Contiene información relevante para la ERS pero que, propiamente no forma parte de la ERS.

Fuente: (IEEE, 2008)

1.4.3. Modelo de Análisis para las aplicaciones web

El análisis contempla cuatro actividades, como indica García Chi (2013):

- Modelado de contenido.
- Modelado de interacción.
- Modelado funcional.
- Modelado de configuración.
- Análisis relación-navegación.

Para la representación de los diferentes modelados usados en el análisis de las aplicaciones web, se utilizará el lenguaje de modelo unificado (UML), el cual ayuda a traducir los requisitos levantados en representaciones de desarrollo de software orientado a objetos (DSOO), modularizando los principales elementos estructurales y de comportamiento y las relaciones entre ellos de una aplicación software. UML permite la modelación tanto de componentes estáticos, así como de componentes dinámicos del software (Vidal, Schmal, Rivero, & Villaroel, 2012).

1.4.3.1. Modelo de contenido

Este modelo contiene los elementos estructurales que son necesarios para satisfacer los requisitos de contenido de la aplicación, como son las clases de contenido. Así como todas las clases de análisis visibles para el usuario que se crean para la interacción con la aplicación. Estas se derivan del análisis gramatical de los casos de uso. (García Chi, 2013)

Las clases de análisis son entidades visibles por el usuario, y son representadas mediante del diagrama de clases de UML, siguiendo los conceptos presentado por el autor.

Diagramas de clases

Definir las clases de un sistema es la tarea más importante dentro de la programación orientada a objetos. La clase es una categoría o agrupación de cosas que tienen propiedades (atributos) y acciones similares (métodos). Los diagramas de clase describen la estructura estática de un sistema y no muestran ningún procesamiento en especial, además indica cómo se relacionan las clases entre sí.

Los elementos que conforman a los diagramas de clase son:

Clase: es un rectángulo dividido en tres secciones, la primera sección contiene el nombre de la clase, la segunda sección contiene los atributos de la clase, los cuales pueden ser públicos (+), protegidos (#) y privados (-) y finalmente en la tercera sección, contiene los métodos o acciones que tiene la clase que al igual que los atributos estos pueden ser públicos, privados y protegidos.

Ilustración 1: Ejemplo de clase.
Fuente: Elaboración propia.

Asociaciones: las asociaciones se representan relaciones estáticas entre las clases, gráficamente se los representa con una línea en el diagrama de clases, es el tipo de relación más simple.

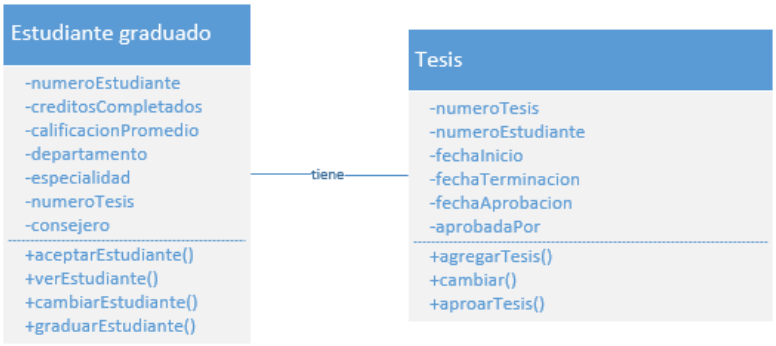

Ilustración 2: Ejemplo asociación.
Fuente: Elaboración propia.

Multiplicidad: son símbolos que se colocan en cada extremo de las asociaciones y representan el número de instancias de una clase vinculadas al número de instancias de la otra, los tipos de multiplicidad son:

- 1, solamente uno.
- 0..1, cero o uno.
- *, muchos.
- 0.. *, cero o muchos.
- 1.. *, uno o muchos.

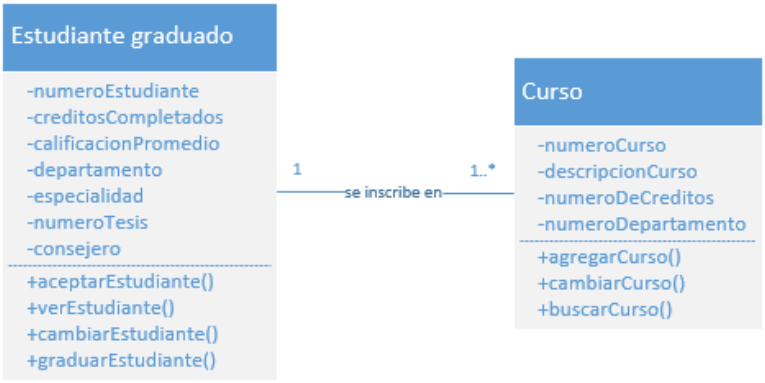

Ilustración 3: Ejemplo de Multiplicidad.
Fuente: Elaboración propia.

Composición y agregación:

La agregación se describe como una relación "tiene un", la agregación hace referencia a que un objeto está compuesto por la suma de sus partes, es una relación más débil, si una clase se elimina la otra puede seguir existiendo. Se lo representa gráficamente con un rombo vacío.

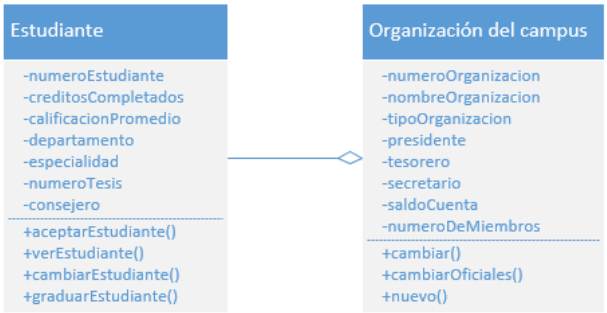

Ilustración 4: Ejemplo de agregación de clases.
Fuente: Elaboración propia.

La composición es una relación fuerte entre el todo y cada una de sus partes, en esta relación una clase "siempre contiene" a otra clase, si la clase todo se elimina la clase parte también desaparecería. Esta relación se la representa gráficamente con un rombo pintado.

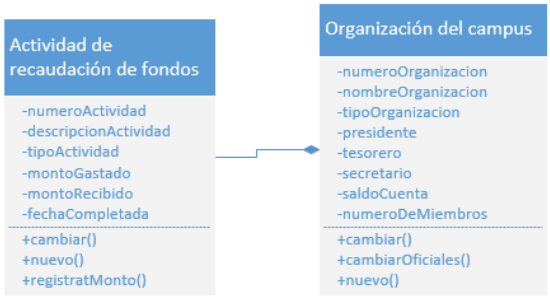

Ilustración 5: Ejemplo composición de clases.
Fuente: Elaboración propia.

Generalización o herencia: es una relación que se refiere a que una clase es la especialización o detalle de una clase más general, gráficamente se lo representa como un triángulo vacío.

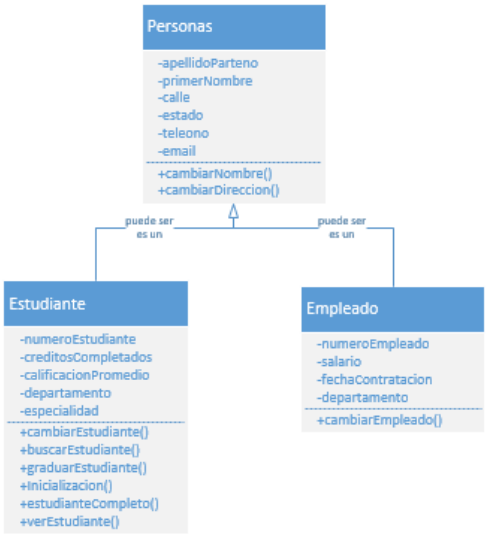

Ilustración 6: Ejemplo de generalización de clases.
Fuente: Elaboración propia.

1.4.3.2. Modelo de interacción

El diagrama de secuencia sirve para representar la interacción que tiene el software con el usuario. Se presentará el diagrama de secuencia siguiendo los conceptos propuestos por Kendall (2011).

Diagramas de secuencia

Es la representación de abreviada de la forma como interactúan las acciones del usuario con las clases, a través del tiempo. Estos diagramas derivan del análisis previo de los casos de uso del software, y utilizan para representar las interacciones, las relaciones y los métodos de las clases. Cada caso de uso puede crear un diagrama de secuencia.

Los elementos que conforman estos diagramas son:

Clase, objeto: es un rectángulo colocado en la parte superior del diagrama, utiliza indicadores en el nombre para indicar si representa una clase, un objeto o una clase y un objeto.

- nombreObjeto: representación del nombre de un objeto.
- :clase representación del nombre de una clase.
- nombreObjeto: clase representación del nombre de un objeto en una clase.

Ilustración 7: Ejemplo de nombre de clase u objeto.
Fuente: Elaboración propia.

Línea de vida: son líneas verticales entrecortadas, paralelas a los rectángulos de inicio, representan la presencia del objeto durante el tiempo, es decir su línea de vida, la X significa la terminación de la línea de vida del objeto por ende su destrucción.

Ilustración 8: Ejemplo de línea de vida.
Fuente: Elaboración propia.

Activación: son rectángulos alargados que representan el tiempo necesita un objeto para cumplir una tarea.

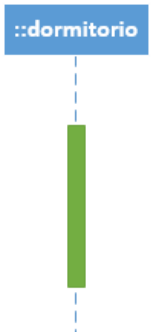

Ilustración 9: Ejemplo de activación.
Fuente: Elaboración propia.

Mensajes: representan la comunicación entre objetos, gráficamente se los representa con flechas.

- → representa un tipo de mensaje simple.

-  representa un tipo de mensaje síncrono, es decir, la clase emisora espera un mensaje de respuesta de la clase receptora.
- representa un tipo de mensaje asíncrono, es decir, la clase emisora no espera un mensaje de respuesta de la clase receptora.
-  representa un tipo de mensaje rechazado.
-  representa un mensaje de time out (tiempo agotado).
- Los mensajes se pueden etiquetar de diferentes formatos:
- Nombre del mensaje entre paréntesis vacíos: nombreMensaje().
- Nombre del mensaje entre paréntesis los parámetros a pasar: nombreMensaje (parámetro1, parámetro2, …).
- Nombre del mensaje entre paréntesis el tipo de dato para el parámetro, el nombre del parámetro y un valor determinado para ese parámetro: nombreMensaje (tipoParámetro: nombreParámentro – (valorPredeterminado)).

Destrucción de objetos: se puede destruir objetos utilizando una flecha que apunta a una X, etiquetado con un mensaje "<<destruir>>".

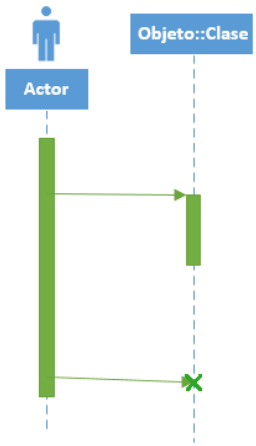

Ilustración 10: Ejemplo de destrucción de objetos.
Fuente: Elaboración propia.

Loops: es la representación de un ciclo repetitivo en un diagrama de secuencia, se coloca la condición para terminar con la repetición entre corchetes [].

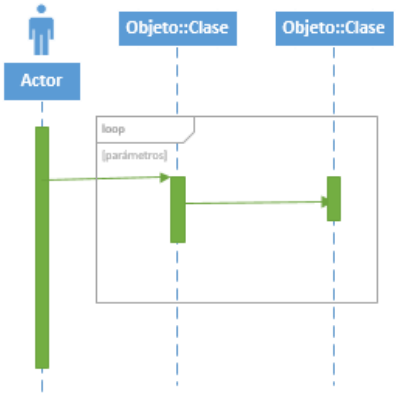

Ilustración 11: Ejemplo de loops
Fuente: Elaboración propia.

1.4.3.3. Modelo funcional

En el modelo funcional se aborda dos elementos como indica García Chi (2013):

- La funcionalidad observable respecto al usuario.
- Las operaciones dentro de las clases de análisis, que representan comportamientos asociados con la clase.

Para la representación del modelo funcional se ocupa el diagrama de actividades. Los conceptos del diagrama de actividades se basan en el autor Kendall (2011).

Diagrama de actividades

Muestran la secuencia (pasos) de actividades de un proceso, en las que se incluyen las actividades en secuencia, paralelas y las decisiones que se toman. Se crea un diagrama de actividad por cada caso de uso que se haya descrito, y muestra los distintos escenarios.

Los elementos que conforman estos diagramas son:

Estados de acción: son rectángulos con las esquinas redondeadas que representan una actividad de un objeto.

Ilustración 12: Ejemplo estado de acción.
Fuente: Elaboración propia.

Flujos de acción: son representaciones de las relaciones entre los estados de las acciones que ocurren en cierto momento y lugar, gráficamente se lo representa con una flecha.

Ilustración 13: Ejemplo de flujos de acción.
Fuente: Elaboración propia.

Estado inicial y final: el estado inicial es desde donde empieza la acción de un objeto, y la final en dónde concluye, al estad inicial se lo representa gráficamente con un circulo pintando y al estado final se lo representa con un círculo pintado dentro de otro.

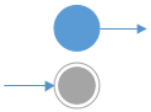

Ilustración 14: Ejemplo de estado inicial y final.
Fuente: Elaboración propia.

Decisión y fusión: la decisión es un diamante sin pintar y representa las decisiones con caminos alternativos, en cada camino debe estar presente el condicionante. La fusión tiene una representación gráfica al de la decisión, sin embargo, representa la fusión de varios eventos para formar un evento.

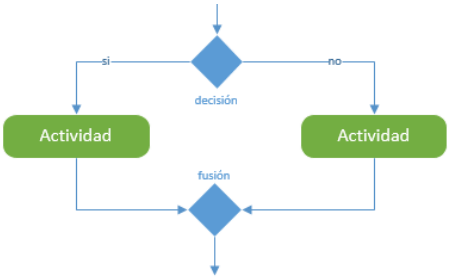

Ilustración 15: Ejemplo de decisión y fusión.
Fuente: Elaboración propia.

Sincronización: un rectángulo plano representa a las barras de sincronización, ayuda a ilustrar la ejecución de actividades paralelas.

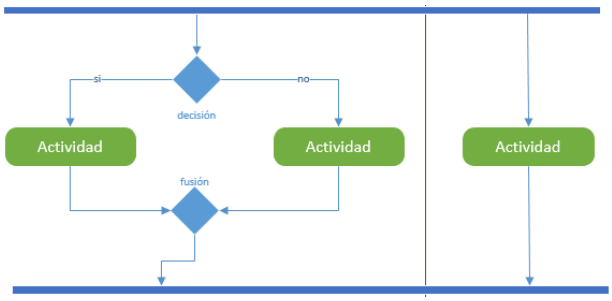

Ilustración 16: Ejemplo de barras de sincronización.
Fuente: Elaboración propia.

Marcos de responsabilidad: agrupan a las actividades que realiza un objeto.

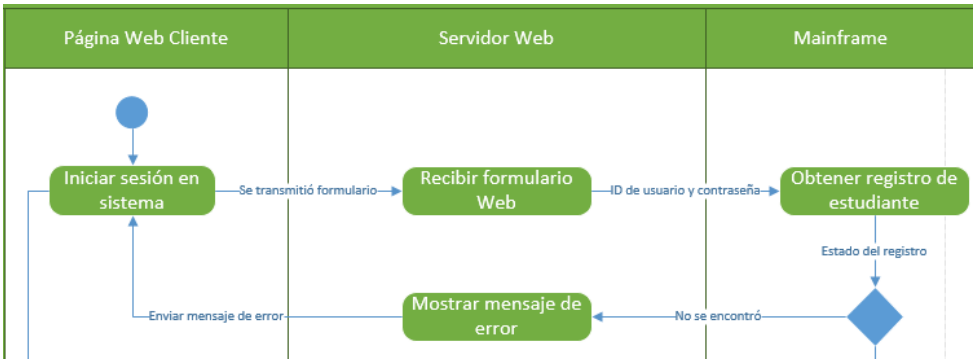

Ilustración 17: Ejemplo marcos de responsabilidad
Fuente: Elaboración propia.

1.4.3.4. Modelo de configuración

Se debe especificar las características de hardware y software soportados, así como también especificar las interfaces bien definidas y seguras para la interacción con las bases de datos y el resto de aplicaciones. (García Chi, 2013)

Para representar el modelo de configuración se utiliza el diagrama de despliegue.

Diagrama de despliegue

El diagrama de despliegue muestra la implementación física del sistema, incluye hardware, y las relaciones entre el hardware y el sistema. El diagrama de despliegue puede representar servidores, estaciones de trabajo, etc. Sirve para modelar la configuración del sistema. (García Chi, 2013)

Los componentes del diagrama de despliegue son:

Nodos: los nodos pertenecen al mundo material, se define como un elemento físico que existe en el tiempo de ejecución y representa un recurso. Dentro del nodo pueden ir los componentes pertenecientes al mismo. (Ferré Grau & Sánchez Segura, 2014)

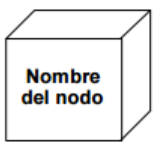

Ilustración 18: Ejemplo de nodo.
Fuente: Elaboración propia.

Asociaciones: es el tipo de relación más común entre los nodos, representa una conexión física entre los mismos. (Ferré Grau & Sánchez Segura, 2014)

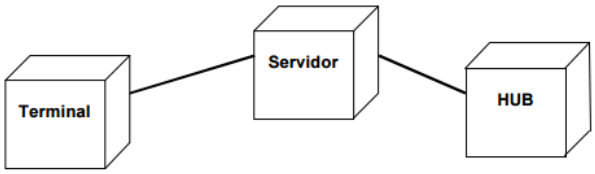

Ilustración 19:Ejemplo Asociación
Fuente: Elaboración propia.

Se han definido ya los elementos de contenido, como de funcionalidad que interactúan con el usuario. Ahora se debe hablar acerca de la navegación cuando se requiere diseñar un software en un entorno web, ya que no se debe tomar a la navegación como simplemente moverse de una página hacia otra, sino debe tomarse como la idea de moverse dentro de un espacio de información. (García Chi, 2013)

Para el análisis, diseño de interfaz y navegación se toman los conceptos planteados por la autora Rosa García (2013).

1.4.3.5. Análisis relación navegación (ARN)

Sirve para determinar la estructura de relación del software. El ARN proporciona una serie de pasos para identificar relaciones entre los elementos.

Pasos de ARN:

- Análisis de los participantes: identificar diversas categorías de usuario.
- Análisis de elementos: se identifica los objetos de contenido y elementos funcionales.
- Análisis de relaciones: se describe las relaciones entre elementos del software web.
- Análisis de navegación: examina como los usuarios pueden acceder a elementos individuales o grupos de elementos.

1.4.4. Modelado de diseño

La interfaz del software debe responder a principios de calidad propios de las aplicaciones Web como: facilidad de uso, funcionalidad, confiabilidad, eficiencia, facilidad de mantenimiento.

1.4.4.1. Metas del diseño

Las metas de diseño son aplicables a todas las aplicaciones Web sin importar el tamaño o su complejidad.

- Simplicidad: tener un contenido moderado y simple.

- Consistencia: el contenido debe guardar la misma apariencia y funcionalidad en todas partes de la aplicación.
- Identidad: se deberá trabajar para establecer una identidad para la aplicación web.
- Robustez: se espera que la aplicación tenga un contenido y una funcionalidad robusta, es decir, que no se rompa.
- Navegabilidad: debe ser simple, consistente, intuitiva y predecible.
- Apariencia visual: debe tener una estética y apariencia visual agradable.
- Compatibilidad: la aplicación puede ejecutarse y ser visto en varias plataformas.

1.4.4.2. Diseño de interfaz

Los siguientes puntos representan el flujo de trabajo para la creación de una interfaz gráfica de la aplicación Web.

1. Revisar toda la información obtenida en el modelo de análisis y mejorarla conforme se requiera.
2. Desarrollar un bosquejo de la plantilla de la interfaz de la aplicación.
3. Correlacionar los objetivos del usuario con acciones específicas de la interfaz.
4. Definir un conjunto de tareas de usuario que estén asociadas a cada acción.
5. Elaborar bosquejos de imágenes en la pantalla para cada acción de la interfaz.
6. Refinar la plantilla de la interfaz con el uso de diseño estético.
7. Identificar los objetivos de la interfaz del usuario.
8. Desarrollar una representación de comportamiento de la interacción del usuario con la interfaz.
9. Revisar el modelo de diseño de la interfaz para confirmar que exista consistencia y facilidad de uso.

1.4.4.3. Diseño estético

Es también llamado diseño gráfico, es la parte artística de la aplicación que complementa los aspectos técnicos de la ingeniería web. Si no se aplicara el diseño estético, la aplicación puede ser funcional, pero sin atractivo.

No existen plantillas absolutas para el diseño estético, sin embargo, se enumeran lineamientos generales:

- No temerle al espacio vacío.

- Resaltar el contenido, el 80% debe ser contenido, el resto debe ser navegación y otras características.
- Organizar los elementos de plantilla de arriba a la izquierda hacia abajo a la derecha, colocado los elementos de mayor importancia arriba a la izquierda.
- Agrupar navegación, contenido y función geográficamente dentro la página.
- Preferiblemente no permitir el uso de barra de desplazamiento de izquierda a derecha.
- Considerar ajustable a dispositivo "Responsive".
- Los medios audiovisuales utilizados deben ser lo más liviano posible para evitar una navegación lenta.
- Considerar agregar efectos como, por ejemplo: efecto Parallax scrolling.

1.4.4.4. Diseño de contenido

El diseño de contenido se enfoca en dos puntos de vista:

- El Ingeniero Web que diseña los objetos contenido y sus relaciones.
- El diseñador gráfico o publicista que se ocupa de la representación de la información del objeto contenido.

Luego del análisis de contenido en el cual se especificaron ciertos atributos de las clases de contenido, se procede con la inserción de atributos específicos de implementación propios del diseño.

1.4.4.5. Diseño Arquitectónico

Se debe identificar la arquitectura de contenido, es decir, cómo se estructura los objetos de contenido para su presentación y navegación en la aplicación web.

Arquitectura de contenido: se centra en la definición de la estructura global de la aplicación web, la arquitectura puede ser basada en diferentes estructuras de contenido.

- Estructura lineal: cuando existe una secuencia predecible de interacciones.
- Estructura en retícula (malla): cuando el contenido está organizado categóricamente en dos o más dimensiones.
- Estructura jerárquica: su flujo de control es vertical por medio de las ramificaciones verticales, pero adicionalmente pueden tener control o flujo horizontal por medio de ramificaciones de hipertexto.

- Estructura de red: está diseñado para poder navegar por medio de vínculos de hipertexto virtualmente a cualquier página del sistema.
- Estructuras compuestas: es una mezcla de las estructuras mencionadas anteriormente.

1.4.4.6. Diseño de navegación

Para este diseño se deben establecer las rutas de navegación que utilizarán los usuarios para acceder al contenido y a las funciones de la aplicación web. Para ello se debe tomar en cuenta la sintaxis y la semántica de la navegación.

Semántica de navegación: se define como el "sentido" de la navegación para los diferentes tipos de usuario, esto se lo toma de las categorías de usuario y se desarrolla un USN (Unidades semánticas de navegación) para cada caso de uso, en los USN se describen los requisitos de navegación, aquí se puede ver como el actor se mueve entre los objetos de contenido y la funcionalidad de la aplicación.

Sintaxis de navegación: se define como la "mecánica" de navegación, teniendo en cuenta varias opciones como:

- Vínculo de navegación: vínculos basados en texto, íconos, botones y metáforas gráficas.
- Barra de navegación horizontal: lista de principales categorías de contenido o funcionales en una barra.
- Columna de navegación vertical: similar a la horizontal con una particularidad que al momento de seleccionar una puede expandir a subcontenidos en forma de árbol.
- Pestañas: es una variación de la barra o columna pero que dan la sensación de marca.
- Mapas de sitio: proporciona una tabla de contenido incluyente para la navegación hacia todos los contenidos y funcionalidad de la aplicación web.

1.4.4.7. Diseño de base de datos

El diseño de la base de datos es importante para una aplicación web, ya que se está estableciendo la estructura en donde se almacenarán los datos que serán importantes para que la aplicación funcione correctamente y cumpla sus objetivos trazados.

Se debe tener claro cuál es el concepto de una base de datos. Las bases de datos son una fuente central de datos con el fin de que los usuarios la compartan para su uso en varias aplicaciones, son gestionadas mediante el administrador de bases de datos (DBMS), el cual permite crear, modificar y actualizar una base de datos. (Kendal, 2011)

Para diseñar una base de datos se utiliza el modelo entidad-relación, la cual representa la estructura lógica global de la base de datos. El modelo entidad-relación se basa en tres conceptos básicos: conjunto de entidades, conjunto de relaciones y atributos. Como lo proponen los autores Silberschatz, Korth, & Sudarshan (2006).

Entidades

Una entidad es una "cosa" u "objeto" del mundo real que sea distinguible de los demás objetos, puede ser de existencia física como una persona, carro, etc. O un objeto de existencia conceptual como una compañía, un trabajo, etc.

Una entidad posee un conjunto de propiedades que pueden hacer que dicha entidad pueda ser identificada de forma unívoca. Un conjunto de entidades es la agrupación de varias entidades que compartes sus mismas propiedades o atributos, por ejemplo, un Cliente.

Atributos

Las propiedades de las entidades conocidas también como atributos describen las características de dicha entidad.

Tipos de atributos:

- Atómico: atributos que no son divisibles, por ejemplo, cédula.
- Compuestos: atributos que son divididos en sub partes, los cuales forman una jerarquía, por ejemplo, dirección puede estar subdividido en país, ciudad, parroquia, barrio, calle.
- Simple valor: atributos que tiene solo un valor, por ejemplo, la edad de una persona.
- Multivalor: atributo que tiene una serie de valores, por ejemplo, una persona tiene varios números de celular.
- Derivados: atributos que pueden derivar de los valores de otros, por ejemplo, cálculo de la edad de una persona a partir de la fecha de nacimiento.
- Llave: es el atributo único por el cual se puede identificar a la entidad individual, por ejemplo, el número de cédula de una persona, es irrepetible.
- Nulos: cuando la entidad no tiene valor para el atributo.

Relaciones

Una relación es una asociación que puede darse entre entidades de la misma clase o de diferentes clases. El grado de las relaciones dependen del número de asociaciones entre clases,

relaciones unitarias (entidades de la misma clase), relaciones binarias (relaciones entre clases), etc. El modelo entidad-relación permite relaciones de cualquier grado.

Propiedades de las relaciones

Roles de una relación: hace referencia a las funciones que desempeñan cada una de las clases de entidades asociadas, por ejemplo, cuando se relacionan la clase A con la clase B, se debe tener en cuenta qué función tiene A en B, y cual B en A.

Cardinalidad de una relación: es el número de entidades de una clase que pueden relacionarse a una entidad de otra clase.

- Relación 1 a 1.
- Relación 1 a N (Varios).
- Relación N (Varios) a 1.
- Relación N (Varios) a N (Varios).

Participación de un conjunto de entidades: indica si todas las entidades de una clase se relacionan necesariamente con las entidades de otra clase asociada. Se considera participación total, si cada entidad de una clase participa en al menos una relación. La participación es parcial cuando alguna entidad de una clase participa en alguna relación.

Dependencia de existencia: si una entidad A depende de una entidad B, entonces, se dice que A depende de la existencia de B. Si se llegase a suprimir la entidad B, también se eliminaría la entidad A.

Con los conceptos propuestos del modelo entidad-relación se puede realizar un diagrama entidad-relación y modelar la base de datos, que será implementada para la construcción de la aplicación web.

Una vez concluido la fase de análisis y diseño de la aplicación, se debe pensar en cómo será el desarrollo del mismo, es decir, se debe establecer como proyecto el desarrollo de la aplicación, y se debe poner en práctica la gestión de proyectos.

1.5. Gestión de proyectos

Una vez que se concluye con las etapas de análisis y diseño de la aplicación software de la metodología Ecu@Risk, se pretende dar una visión acerca del desarrollo del software en sí, es

decir, gestionar el proyecto de desarrollo del software, para eso es necesario entender ¿Qué es un proyecto?, ¿Qué es la gestión?, y finalmente ¿Qué es la gestión de proyectos?

1.5.1. ¿Qué es un proyecto?

La definición de proyecto según el *Project Management Institute* (PMI) "es un esfuerzo temporal que se lleva a cabo para crear uno producto o servicio único", es decir, es una combinación de diversos factores tanto humanos, tecnológicos, financieros, etc., los cuales unen esfuerzos para llevar a cabo un conjunto de actividades en un tiempo y espacio determinado, que les permitan la consecución de objetivos marcados, la forma de terminar un producto, desarrollo de un servicio único, ya que de alguna manera deben ser diferentes. (Gómez Rueda, 2016)

Según Gómez Rueda (2016) las características básicas de un proyecto son:

- Temporalidad: tiene un comienzo y un fin marcados.
- Entregables: se refiere a los documentos con los resultados generados de la realización del proyecto, también son los productos o servicios.
- Objetivo: se refiere al entregable o entregables que forman parte del objetivo para realizar el proyecto.
- Contexto: pueden ser de larga duración y ser la influencia externa o interna del proyecto.
- Restricciones: son las partes que pueden influir en la realización del proyecto.
- Riesgo e incertidumbre: son eventos que tienen un cierto grado de probabilidad de influir en el proyecto de manera negativa.
- Ciclo de vida: son las etapas en el cual se desarrolla el proyecto, comenzando por la definición y haciéndose más explícito y detallado conforme el proyecto avanza, culminando cuando el producto o servicio se desarrolló se retira o se da de baja.

1.5.2. ¿Qué es la gestión?

La gestión según la definición de la Real Academia Española es "la acción y efecto de gestionar", y la definición de gestionar es "hacer diligencias contundentes al logro de un negocio o de un deseo cualquiera", es decir, realizar actividades definidas, controladas y organizadas para conseguir un objetivo planteado.

Las funciones de la gestión según Gómez Rueda (2016) son:

- Planificar: se determina qué resultados se van a obtener y las estrategias que se van a aplicar para su realización.
- Organizar: se especifica cómo lograr los resultados planificados, asignando tareas a los miembros y equipos que estén involucrados para que se alcancen los objetivos planteados.
- Controlar: comprobar si lo que se ha planificado se está alcanzando con los resultados previstos, se deben corregir todas las desviaciones y contratiempos que se presenten.
- Dirigir: liderar y motivar a los miembros y equipos involucrados, de tal manera que se cumpla y se alcance todo lo que se ha planificado.

1.5.3. ¿Qué es la gestión de proyectos?

Una vez que se ha definido un el concepto de proyecto y gestión, es conveniente tratar la Gestión de proyectos; la definición de Gómez Rueda (2016) acerca de la dirección y gestión de proyectos es el uso de conocimientos, métodos, herramientas, técnicas y competencias a las actividades de un proyecto con la finalidad de satisfacer sus requisitos y por consecuencia obtener los resultados deseados.

Gómez Rueda (2016) indica que a gestión de proyectos no es un proceso que sea totalmente definido, debido a que muchas personas y organizaciones que lleven a cabo un proyecto se pueden tener distintos enfoques, por ejemplo, unos pueden valorar más el control y seguimiento, mientras que otros se enfocan en el liderazgo y en las personas, etc. Así mismo se presentan diferentes metodologías tradicionales y ágiles, con diferentes enfoques al momento de elaborar el proyecto.

Se debe escoger el enfoque que mejor se adapte al desarrollo del proyecto y a la organización o persona que lo vaya a desarrollar.

1.5.4. ¿Por qué la gestión de proyectos?

Los estudios realizados desde hace algunos años revelan que para que los proyectos informáticos lleguen a una correcta y exitosa culminación es necesario que exista una gestión integral del proyecto que abarque todo su ciclo de vida, es decir, desde la visión e idea hasta el cierre formal del mismo.

Los beneficios que trae gestionar un proyecto según Gómez Rueda (2016) son:

- Ahorros de tiempo y coste: la aplicación de metodologías de gestión de proyectos ahorra tiempo y dinero porque tienen procesos ya definidos que pueden ser utilizados y adaptados.
- Más rapidez en la resolución de problemas: la planificación y gestión de incidencias ayuda a asegurar que los problemas sean resueltos tan rápido como sea posible.
- Optimización en la resolución de riesgos: todos los marcos y modelos de gestión de proyectos incluyen procesos para identificar y gestionar riesgos.
- Mayor efectividad en la comunicación y gestión de expectativas: muchos de los problemas que se presenten en los proyectos pueden ser solucionados con una correcta comunicación multidisciplinar.
- Mayor calidad de productos y servicios: es resultado de la implementación de controles de calidad y técnicas de aseguramiento de la calidad.
- Mejora del ambiente laboral: cuando el proyecto finalice, se encontrarán beneficios en los grupos de trabajo, más unidos, más comprometidos, etc.

Es muy importante introducir en el proyecto que se vaya a desarrollar una gestión del mismo porque va a garantizar que el resultado final sea exitoso y cumpla con las expectativas trazadas en él.

1.6. Conclusiones capítulo 1

Ante el crecimiento de las tecnologías de la información, las empresas deben proteger y asegurar su información de una manera segura y eficaz, debido a que, la información se ha convertido en pieza clave y fundamental en sus labores diarias. La gestión de riesgos ayuda a las empresas a identificar sus vulnerabilidades y qué riesgos podrían atacarlos, también a evaluar e identificar los riesgos a ser tratados, transferidos y aceptados, para finalmente implementar planes de mitigación hacia los riesgos y así proporcionar seguridad en que la información de la empresa no se verá afectada y por consecuencia la empresa no afectará su desempeño.

Ecu@Risk es una metodología de gestión de riesgos de información que se adapta al entorno de la micro, pequeña y mediana empresa (MPYMES), desarrollada bajo una serie estándares y marcos de gestión internacionales, mismo que es aplicable a la realidad de las empresas ecuatorianas. El fin de la metodología es facilitar la gestión de riesgos a las empresas sin las exigencias ni complejidad de otras metodologías de gestión.

Las directrices para la elaboración de un software SGSI parte con los conceptos y aplicación de la ingeniería de software, misma que tiene varias ramas, una de ellas es la orientada a los sistemas y aplicaciones en la red llamada “ingeniería web”, en la cual se facilitan modelos para el análisis de las necesidades de software, el diseño del mismo, también la codificación, implementación y documentación. Cada aspecto de la ingeniería del software es muy importante y siempre debe estar dirigida y pensada hacia el usuario final; desde el levantamiento de los requerimientos hasta terminar con la implementación y documentación del mismo.

Posterior a la definición de las directrices para la elaboración del software, se toma a la codificación, implementación y documentación del sistema de gestión de seguridad de la información como un proyecto, el cuál debe definir un plan, un cronograma, un presupuesto, etc., por este motivo, los conceptos de la gestión de proyectos serán aplicados en el desarrollo de del software. La gestión de proyectos requiere un presupuesto el cual se desarrolla a partir del análisis de las directrices del futuro software. El desarrollo de un proyecto siempre está propenso al surgimiento de cualquier inconveniente que pueda afectar su normal desarrollo, es por ello que se elabora un plan de gestión de riesgos de proyectos, el cual pueda brindar ayuda a prevenir o solucionar algún percance que pueda surgir ante el desarrollo del proyecto.

Todos los conceptos repasados en el desarrollo del primer capítulo de este documento serán aplicados a lo largo del desarrollo de las siguientes secciones, todos estos conceptos conforman la base teórica en la cual respalda el desarrollo de las directrices para la elaboración del sistema de gestión de seguridad de información, el cual aplicará la metodología Ecu@Risk para las empresas MYPES.

Capítulo 2: Análisis de la metodología Ecu@Risk

2.1. Introducción

Se analizará la metodología de gestión de riesgos de información Ecu@Risk, partiendo con el marco de gestión de riesgo de la metodología, continuando con todos los procesos de gestión de riesgo y finalmente se describirán los recursos que utiliza la metodología para su aplicación, lo que permitirá posteriormente definir los procesos, procedimientos y opciones que deberá contener el software.

2.2. Marco de gestión de riesgo

Cualquier metodología de gestión de riesgo debe integrar todos los procesos que permitan administrar el riesgo en todos los niveles de gobierno institucional, conjuntamente con la planeación y estrategias. (Crespo, 2016)

La metodología Ecu@Risk identifica roles y responsabilidades que el personal debe obtener y considerar en el proceso de gestión de riesgo, para que el marco de gestión de riesgo de la metodología sea efectivo.

En la metodología Ecu@Risk de Crespo (2016), se propone los siguientes roles, los cuales estarán involucrados para la correcta aplicación de la misma.

Alta dirección: dentro de cualquier tipo de organización, la alta dirección debe asegurarse de proporcionar los recursos necesarios para desarrollar las capacidades necesarias que permitirán llevar a cabo la misión. Además, estará a cargo de la evaluación de riesgos, así como, en la toma de decisiones. Es un actor clave para en la gestión de riesgos.

Propietarios de información: son los responsables de gestionar la información, así como aprobar el acceso a la misma, validando controles establecidos, con el fin de garantizar la confidencialidad e integridad de la información. En general, el propietario de la información es el gerente, subgerente o jefe de área.

Propietario(s) de sistemas de información: es o son los responsables de implementar y asegurar los controles que se hayan elegido estén funcionando, para garantizar la integridad, disponibilidad y confidencialidad de los sistemas de información y de los datos que poseen. Generalmente es el técnico encargado de sistemas, o el jefe de departamento de TI.

Comité de Riesgo de Tecnología de Información (CRTI): tienen la responsabilidad de evaluar la planificación de riesgo tecnológico y de información, monitorear la gestión del rendimiento, incluyendo los componentes de seguridad de la información. Las decisiones que se tomen dentro de esta área deben estar sujeto al programa de gestión de riesgo.

Coordinador de Seguridad designado (CSD): el coordinador de seguridad de información es responsable designado por el CRTI para los programas de seguridad de la organización, la cual incluye a la gestión de riesgos. Tiene un papel muy importante dentro de la identificación, evaluación y minimización de los riesgos de los sistemas informáticos de la organización. El CSD actúa también como consultor principal en apoyo de la alta gestión para asegurarse de que esta actividad se lleve a cabo de manera continua. No puede ser parte del departamento o el área de TI por razones éticas y por funciones incompatibles.

Profesionales de TI – Proveedores de soluciones técnicas (PST): son conformados por profesionales de TI, son responsables de la correcta aplicación de los requisitos en su sistema TI.

Auditor de TI: vela por el cumplimiento de las políticas, las normativas y el control de los servicios de TI, determinando si estos son adecuados y permiten alcanzar los objetivos y estrategias planteadas por la organización.

Comité de certificación de TI: los cambios producidos en el sistema de información, los Profesionales de TI y los miembros del comité de riesgos de TI, deben validar los cambios realizados, identificar y evaluar nuevos riesgos que se puedan presentar, para actuar según sea conveniente.

2.3. Proceso de gestión del riesgo

En el mundo actual cualquier gestión de riesgo es cada vez más necesaria para cualquier aspecto de la vida cotidiana, como, por ejemplo: tomar una decisión, iniciar un proyecto, etc. Es así como en una organización MPYME es necesario implementar procesos que gestionen los riesgos, ya que facilitan la identificación, análisis, tratamiento y mitigación de los mismos, los cuales se encuentran latentes en el entorno de desarrollo de la empresa.

La gestión de riesgo manejada por la metodología Ecu@Risk se basa en el modelo de Deming, el cual tiene cuatro etapas, las mismas que son descritas por el autor Mendoza (2015).

Planificar: en esta etapa se definen los objetivos y medios para conseguirlos.

Ejecutar: se trata de implementar lo que se haya planificado anteriormente.

Verificar: comprobar que se alcancen los objetivos previstos y con los recursos asignados.

Actuar: consiste en analizar y corregir los problemas que se detecten.

Crespo (2016) indica que la metodología de gestión de riesgos de información Ecu@Risk se resume en cinco procesos de gestión, un proceso de monitoreo y control y finalmente un proceso comunicacional. Para el desarrollo del software que requiere la metodología se centrará el análisis en los procesos de gestión de la metodología, las cuales se describirán a continuación.

2.3.1. Identificación de los activos de información

Los activos de información hacen referencia a cualquier tipo de elemento que contenga información y sea utilizado para la empresa u organización, por ejemplo: base de datos, contratos, software, etc. La metodología Ecu@Risk plantea los siguientes activos de información, clasificados en diferentes grupos:

Tabla 3:
Grupos de clasificación de activos de información.

(ED)	Edificaciones
(HW)	Hardware
(SW)	Software
(IE)	Información electrónica
(IP)	Información en papel
(Extraíble)	Medios de almacenamiento extraíble
(IC)	Infraestructura de comunicaciones
(RRHH)	Recursos humanos

Fuente: (Crespo, 2016)

El proceso de identificación de los activos de información que sugiere la metodología es el siguiente:

- Identificar los procesos de negocio de la organización.
- Evaluar los elementos de información según las clasificaciones de los activos que intervienen en el mismo.

- Registrar los activos de información según las directrices que se indica en la metodología.

Para realizar la identificación de acuerdo a la clasificación, la metodología Ecua@Risk de Crespo (2016) divide a cada grupo en diferentes categorías, las mismas que se describirán a continuación.

2.3.1.1. Clasificación de activos de información

Edificaciones

Tabla 4:
Clasificación de Edificaciones.

(ED)	**Edificaciones**		
Clasificación		**Sub clasificación**	**Observaciones**
(CDP)	Centro de cómputo principal		Generalmente las micro y pequeñas empresas cuentan con uno o dos servidores de aplicaciones, las cuales se encuentran ubicados usualmente en el área administrativa. En una mediana empresa el centro de cómputo usualmente es un cuarto independiente.
(CPA)	Centro de procesamiento alterno		
(AT_CLI)	Espacio público de atención al cliente		
(CONTA)	Área de contabilidad		
(SEN)	Área restringida (o áreas sensibles, hace referencia a lugares en la edificación a las cuales su acceso es restringido o limitado o puede estar sujeta a restricciones)	**Hospital:** - (QUI) Quirófano - (UCI) Unidad de cuidados intensivos - (RAYX) Unidad de rayos X - (TOMOGRAFIA) Unidad de tomografía - (FARM) Farmacia - (CAJA) Área de cajas - (EME) Área de emergencias	

		- (PED) Área de pediatría - (NEO) Área de Neonatología - (OTRO) Otras áreas sensibles **Entidades financieras:** - (ET) Emisión de tarjetas - (BOVEDA) Bóveda de valores - (CAJA) Área de cajas - (CTE) Área de procesamiento de cámara (cheques) - (OTRO) Otras áreas sensibles **Entidades comerciales:** - (BDG) Bodega - (CAJA) Área de cajas - (OTRO) Otras áreas sensibles **Entidades industriales:** - (PLANTA) Planta de producción - (BDG) Bodega - (TALLER) Espacio para taller de construcción y/o reparación - (OTRO) Otras áreas sensibles **Entidades educativas:** - (DIR) Dirección - (COCINA) Área de cocina - (AULA) Aulas - (PF) Área de atención a padres de familia.	
(GER)	Gerencia		
(FIN)	Área financiera		
(VENTAS)	Área de ventas		
(SEG)	Área de seguridad y vigilancia		

(OTRO)	Otras áreas no contempladas		Describir las áreas no contempladas utilizando codificación adicional para cada espacio que no se haya considerado en este documento, EJ: (OTRO)(MRK), hace referencia al área de Marketing.

Fuente: (Crespo, 2016)

Para la codificación del activo de información, Crespo (2016) indica que debe estar estructurada de la siguiente manera:

(Cod. Clasificación del activo) (Sub código) (Sub código) (Secuencial)

El campo secuencial es un número incremental que sirve para distinguir activos de información del mismo tipo.

Una vez revisada las categorías de las edificaciones un ejemplo para referirse al aula 1 de una entidad educativa, la codificación del activo sería:

(ED) (SEN) (AULA) (01)

Crespo (2016) considera si algún área sensible de algún tipo de industria no esté contemplada en el documento, por ejemplo, la industria comida (restaurantes, bares, tenedores), se recomienda seguir el siguiente procedimiento:

1) Identificar el área y colocar una nomenclatura de acuerdo con la organización:
    a. (CLI): Área de clientes
    b. (COCINA): Área de cocina
    c. (CAJA): Área de cajas y cobros
2) Establecer la codificación
    a. (ED) (SEN) (CAJA) (01)
3) Con ello se tiene que la codificación hace referencia a una caja que se encuentra en el restaurante.

Hardware

El Hardware hace referencia a la parte física de una computadora o un sistema informático, en la metodología se clasifica de la siguiente manera.

Tabla 5:
Clasificación de Hardware.

(HW)	**Hardware**		
Clasificación		**Sub clasificación**	**Observaciones**
(SRV)	Servidores		Se considera un equipo servidor a un equipo de coste económico medio, tanto en adquisición como en su mantenimiento.
(PC)	Equipos de escritorio		Se considera como PC a los computadores de bajo costo económico y que son de fácil reemplazo.
(LAPTOP)	Computadores portátiles		
(CELULAR)	Teléfonos celulares no inteligentes		
(SMART)	Teléfonos celulares inteligentes		Es considerado un teléfono inteligente si tiene la capacidad de navegar por internet, gestionar aplicaciones, gestionar documentos. Usualmente con un sistema operativo Android, iOS o Windows.
(PRINT)	Impresoras		
(SCAN)	Escáneres		
(MULTI)	Impresoras multifuncionales		Una impresa multifunción es aquella que tiene la capacidad de imprimir y escanear.
(FAX)	Sistemas de transmisión FAX		
(FW)	Firewall		

Fuente: (Crespo, 2016)

La manera de codificar se mantiene como se detalló anteriormente.

Software

El Software son las aplicaciones, programas informáticos, sistemas operativos, antivirus, navegadores de internet, etc. Todo lo que permite a la computadora o sistema informático realizar determinadas tareas. La metodología clasifica al software de la siguiente manera.

Tabla 6:
Clasificación de Software.

(SW)	**Software**		
Clasificación		**Sub clasificación**	**Observaciones**
(Propio)	Desarrollo propio		Software que ha sido desarrollado dentro de la propia empresa. Lo que se busca es asegurar su código fuente y propiedad intelectual.
(SUB)	Desarrollo subcontratado		Software que ha sido elaborado para la empresa por terceros.
(STD)	Software estándar		Software comercialmente adquirido. (ver subclasificación siguiente)
	(OFI)	Paquetes ofimáticos	Programas de Office, entre otros pueden ser considerados como ofimáticos.
	(CLIEMAIL)	Cliente de correo electrónico	Puede ser considerado Outlook, Entourage.
	(SRVMAIL)	Servidor de correo electrónico	Usualmente es provisto por terceros como Gmial, Hotmail, etc.
	(OS)	Sistema operativo	Sistemas operativos como Windows, Linux, etc.
	(AV)	Antivirus	
	(BACKUP)	Respaldos	Sistemas de respaldos de información
	(DBMS)	Gestor de base de datos	Gestores de base de datos como: Oracle, MySQL, SQL Server, Access.

Fuente: (Crespo, 2016)

Información electrónica

La metodología Ecu@Risk indica que se considera información electrónica a los archivos electrónicos, ya sean resultado del manejo de una hoja de cálculo, de un documento de texto, de una fotografía, un registro de base de datos, etc. Se indicará la clasificación de información electrónica a continuación.

Tabla 7:
Clasificación de Información electrónica.

(IE)	**Información electrónica**		
Clasificación		**Sub clasificación**	**Observaciones**
(ARCHIVO)	Archivos		Es considerado archivo a cualquier documento electrónico.
(COPIA)	Archivos de respaldo		Archivos electrónicos de respaldo (copia del original)
(CONF)	Archivos de configuración		
(CLAVE)	Archivos de contraseñas		
(LOG)	Archivos que contienen el registro de actividades		
(EXE)	Código ejecutable		El código ejecutable tiene una extensión EXE, COM o BAT.
(FUENTE)	Código fuente		El código fuente de una aplicación, módulo, componente o sistema.

Fuente: (Crespo, 2016)

Información en papel

En toda empresa existirá información que no sea electrónica. Se debe considerar a la información proveniente de registros de papel, cheques, pagarés, balances, estados financieros, etc. Es decir, cualquier información que no sea electrónica la metodología Ecu@Risk considera como información en papel.

Tabla 8:
Clasificación de Información en papel.

(IP)	**Información en papel**		
Clasificación		**Sub clasificación**	**Observaciones**
(DOCS)	Documentos		Se considera documento a cualquier información que se encuentre en papel.
(CARBON)	Copia carbón del documento		Copia en carbón del documento.

Fuente: (Crespo, 2016)

Medios de almacenamiento extraíble

Esta categoría hace referencia a CDs, DVDs, unidades USB, la metodología los cataloga de la siguiente manera.

Tabla 9:
Clasificación de Medios de almacenamiento extraíble.

(EXTRAIBLE)	**Medios de almacenamiento extraíble**		
Clasificación		**Sub clasificación**	**Observaciones**
(OPTICO)	Medios de almacenamiento óptico		Son medios de cuidado en su almacenamiento, y necesitan un lector óptico para la lectura de la información que contienen.
	(CD)	CD Rom	Medios de almacenamiento de 640 MB hasta 700 MB.
	(DVD)	DVD Rom	Medios de almacenamiento de 4GB hasta 8 GB.
	(BLUE)	BLUE Ray	Medios de almacenamiento de 10 GB.
(ELECTRONICO)	Medios de almacenamiento electrónico		Medios de almacenamiento electrónico cuya interfaz es el USB.
	(PEN)	Pen Drive / Flash Memory	

(MECANICO)	(DISCO)		Medios mecánicos extraíbles: Discos duros externos.

Fuente: (Crespo, 2016)

Infraestructura de comunicaciones

La infraestructura de comunicaciones se refiere a los elementos que permiten la intercomunicación entre los dispositivos informáticos y electrónicos de la red. La clasificación que propone la metodología se presenta a continuación.

Tabla 10:
Clasificación de Infraestructura de comunicaciones.

(IC)	**Infraestructura de comunicaciones**		
Clasificación		**Sub clasificación**	**Observaciones**
(ROUTER)	Router		Dispositivo que es utilizado para la interconexión y salida a una red diferente.
(SWITCH)	Switch		Dispositivo que es utilizado para la interconexión entre computadoras.
(HUB)	Hub		Dispositivo que es utilizado para la interconexión entre computadoras.
(PBX)	Central telefónica		
(VOIP)	Voz sobre IP		Dispositivo de voz sobre IP.
(MODEM)	Módem		Usualmente es un dispositivo que permite acceso a internet.
(WIFI)	Red WiFi		Red inalámbrica (sin cables).
(LAN)	Red LAN		Red de área local (red cableada).

Fuente: (Crespo, 2016)

Recursos humanos

Finalmente, la última categoría que toma en cuenta la metodología es Recursos humanos, la cual hace referencia al personal que forma parte de las actividades de la empresa. La clasificación que sugiere la metodología es la siguiente.

Tabla 11:
Clasificación de Recursos humanos.

(RRHH)	**Recursos humanos**		
Clasificación		**Sub clasificación**	**Observaciones**
(UE)	Usuario externo		Usuario externo de la empresa, ej: proveedores, clientes.
(UI)	Usuario interno		Personal de la empresa.
(TI)	Personal de TI		Personal del área de tecnologías de la información.

Fuente: (Crespo, 2016)

Dimensiones de valoración

Una vez que el activo de información haya sido clasificado y codificado de acuerdo a las categorías anteriores, el siguiente paso es valorar a dicho activo de acuerdo a las dimensiones de valoración.

Crespo (2016) en su metodología indica que las dimensiones de valoración son las características o atributos que hacen valioso a un activo. Una dimensión se considera a un aspecto del activo de información que puede ser independiente de otros aspectos, con lo cual se puede realizar un análisis de riesgos enfocándose en un aspecto, independientemente del resto.

La valoración se utiliza para evaluar las consecuencias de que una amenaza llegue a cumplirse, es decir, la valoración es la medida de perjuicio para la empresa u organización si el activo llega a ser dañado en la dimensión evaluada. (Crespo, 2016)

La metodología muestra las dimensiones a tomar en cuenta:

[D] Disponibilidad

Propiedad o característica de los activos en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

¿Qué pasaría si la información de los activos no se encuentra disponible cuando se la necesita?

[I] Integridad

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]

¿Qué pasaría si la información o los datos de los activos se modifiquen sin control ni conocimiento?

[C] Confidencialidad

Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]

¿Qué pasaría si la información que contienen los activos es conocida por personas u organizaciones no autorizadas?

2.3.1.2. Criterios de valoración

Una vez que se haya determinado las dimensiones de valoración, el siguiente paso es valorar al activo de acuerdo a un criterio de valoración.

Crespo (2016), en la metodología Ecua@Risk define unas normas a seguir para la valoración:

Usar una escala común de valoración para todas las dimensiones, esto permite comparar riesgos.

Usar una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas.

Utilizar un criterio homogéneo que permita comparar los análisis realizados por separado.

Ecu@Risk propone los siguientes criterios de valoración:

Tabla 12:
Criterios de valoración.

valor	criterio	
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor

0	despreciable	irrelevante a efectos prácticos

Fuente: (Crespo, 2016)

2.3.1.3. Registro de activos de información

Para cada registro de información de deberá considerar, al menos:

Código del activo	Descripción	(D)	(I)	(C)	Valoración total	Valor

En el campo "Valoración total" se registrará el valor más alto de la fila, es decir el valor más alto entre la Disponibilidad (D), Integridad (I) y Confidencialidad (C), finalmente para el campo "Valor" se utilizará la tabla de criterio de valoración, comparándolo con el valor del campo "Valoración total", por ejemplo:

Código del activo	Descripción	(D)	(I)	(C)	Valoración total	Valor
(HW) (PC) (01)	Equipo de atención al cliente	5	9	4	9	**Muy alto**

Se supone que se evalúa una entidad financiera y uno de sus procesos de negocio es la "Atención al cliente en ventanilla" con dos subprocesos de negocio:

- "Recepción de valores de depósito".
- "Pagar valores solicitados en retiro de efectivo".

Para el proceso de "Atención al cliente en ventanilla" y sus dos subprocesos asociados se debe considerar: un equipo servidor, mismo que cuenta con sistema operativo Windows Server 2012, una base de datos MySQL y el aplicativo utilizado en la ventanilla, mismo que ha sido desarrollado por terceros, al igual que un operador del sistema, un administrador del sistema, también se requiere un espacio físico en donde se encuentre alojado el servidor.

Entonces se hablaría de los siguientes activos para el proceso de negocio:

Activo	**Descripción**
Hardware	Equipo servidor
Software	Sistema Operativo Windows 2012
Software	Aplicativo de ventanilla
Software	Base de datos MySQL

Información electrónica	Registro de la base de datos de clientes
Información electrónica	Registro de la base de datos de cuentas
Información electrónica	Registro de la base de datos movimientos
Edificaciones	Centro de cómputo principal
Recursos humanos	Administrador del sistema
Recursos humanos	Operador de sistemas

La identificación de los procesos y subprocesos conjuntamente con sus respectivos activos siguiendo la metodología Ecu@Risk quedaría de la siguiente manera:

Proceso	Subproceso	Activo	Descripción
Atención al cliente en ventanilla	Recepción de valores de depósito	(HW)(SVR)(001)	El equipo servidor
		(SW)(STD)(OS)(001)	Sistema Operativo Windows 2012
		(SW)(SUB)(001)	Aplicativo de ventanilla
		(SW)(STD)(DBMS)(001)	Base de Datos MySQL
		(IE)(DATA)(001)	Registros de la base de datos de cuentas
		(IE)(DATA)(002)	Registros de la base de datos clientes
		(IE)(DATA)(003)	Registros de la base de datos movimientos
		(ED)(CPD)(001)	Centro de cómputo principal
		(RRHH)(TI)(001)	Operador de sistemas
		(RRHH)(TI)(002)	Administrador del sistema
	Pagar valores solicitados en retiro de efectivo	(HW)(SVR)(001)	El equipo servidor
		(SW)(STD)(OS)(001)	Sistema Operativo Windows 2012
		(SW)(SUB)(001)	Aplicativo de ventanilla
		(SW)(STD)(DBMS)(001)	Base de Datos MySQL
		(IE)(DATA)(001)	Registros de la base de datos de cuentas
		(IE)(DATA)(002)	Registros de la base de datos clientes

		(IE)(DATA)(003)	Registros de la base de datos movimientos
		(ED)(CPD)(001)	Centro de cómputo principal
		(RRHH)(TI)(001)	Operador de sistemas
		(RRHH)(TI)(002)	Administrador del sistema

2.3.2. Identificación de amenazas

Para la metodología, un punto muy importante es la identificación de amenazas que pueden afectar la organización, por lo tanto, se propone un catálogo de amenazas posibles sobre los activos de información, para cada amenaza se presenta una tabla como la siguiente:

Tabla 13:
Identificación de amenazas.

[código] descripción resumida de lo que puede pasar	
Tipos de activos: Que activos se pueden ser afectados por este tipo de amenazas.	**Dimensiones:** Enumerar las dimensiones de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenar de menor a mayor relevancia.
Descripción: una explicación complementaria o más detallada de la amenaza, y lo que puede ocurrir con los activos del tipo indicado con sus respectivas consecuencias.	

Fuente: (Crespo, 2016)

Según un estudio realizado por Crespo (2016), en el Ecuador las amenazas organizacionales pueden ser clasificadas en:

- Riesgos naturales.
- Riesgos provocados (deliberados).
- Riesgos provocados (por error).
- Riesgos informáticos.
- Riesgos comunicacionales.

La metodología Ecu@Risk explica cada uno de los desastres provocados por cada uno de los riesgos en las siguientes tablas:

Desastres causados por riesgos naturales, donde el hombre no tiene intervención.

[NATURALES] Errores y fallos no intencionados

Tabla 14:
Desastres naturales.

[N.*] Desastres naturales	
Activos afectados: [HW] Equipos informáticos, [EXTRAIBLE] Soportes de información, [ED] Edificaciones, [RRHH] Recursos humanos	Dimensiones: 1. [D] Disponibilidad
Descripción: incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, incendios e inundaciones.	

Fuente: (Crespo, 2016)

Desastres causados a propósito realizados de forma deliberada.

[PROVOCADO] Errores y fallos no intencionados.

Tabla 15:
Desastres provocados.

[PROVOCADO. *] Desastres provocados	
Activos afectados: [HW]Equipos informáticos, [EXTRAIBLE] Soportes de información, [ED] Edificaciones	Dimensiones: 1. [D] Disponibilidad
Descripción: desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, corte energético, accidentes de tránsito, construcción, vibraciones, polvo, suciedad, temperatura, humedad, incendio e inundación. Origen: Entorno (accidental) Humano (accidental o deliberado).	

Fuente: (Crespo, 2016)

Considerando las especificaciones de Crespo (2016), los fallos no intencionales causados por personas, pueden provocar ataque deliberados. Origen: Humano (accidental)

[NO_INTENCIONADO] Errores y fallos no intencionados

Tabla 16:
Errores y fallos no intencionados.

[NO_INTENCIONADO.1] Errores de los usuarios	
Activos afectados: [IE] Información electrónica, [IP] Información en papel, [SW] Aplicaciones (software),	**Dimensiones:** 1. [I] Integridad, 2. [C] Confidencialidad, 3. [D] Disponibilidad

[EXTRAIBLE] Soportes de información	
Descripción: Errores involuntarios de personas cuando usan los servicios, datos, etc.	

Fuente: (Crespo, 2016)

Tabla 17:
Errores del administrador.

[NO_INTENSIONADO.2] Errores del administrador	
Activos afectados: [IE] Información electrónica, [IP] Información en papel, [SW] Aplicaciones (software), [HW] Equipos informáticos, [IC] Infraestructura de comunicaciones	**Dimensiones:** 1. [D] Disponibilidad, 2. [I] Integridad, 3. [C] Confidencialidad
Descripción: Errores involuntarios de personas con responsabilidades de instalación y operación.	

Fuente: (Crespo, 2016)

El hecho de no registrar correctamente las operaciones, sucesos y eventos producidos en la organización, puede ocasionar incidentes, es por eso que la metodología considera los errores de monitorización.

Tabla 18:
Errores de monitorización (log).

[NO_INTENCIONADO.3] Errores de monitorización (log)	
Activos afectados: [IE] Información electrónica, [IP] Información en papel (de cada actividad y registro de errores)	**Dimensiones:** 1. [I] Integridad
Descripción: inadecuado registro de monitorización: falta de recursos, registros incompletos, registro con fechas erróneas, etc.	

Fuente: (Crespo, 2016)

Cuando no se configura bien un dispositivo, ya sea por descuido o negligencia, puede verse afectado este activo; por lo que se debe considerar.

Tabla 19:
Error de configuración.

[NO_INTENCIONADO.4] Error de configuración	
Activos afectados: [IE] Información electrónica, [IP] Información en papel	**Dimensiones:** 1. [I] Integridad
Descripción: introducción de datos de configuración erróneos.	

Fuente: (Crespo, 2016)

La metodología también hace referencia a deficiencias en la organización.

Tabla 20:
Deficiencias en la organización.

[NO_INTENCIONADO.5] Deficiencias en la organización	
Activos afectados: [P] Personal	**Dimensiones:** 1. [D] Disponibilidad
Descripción: cuando no están bien definidas las funciones de cada persona en la organización, incluyendo tomar medidas sobre activos. Acciones descoordinadas, errores por omisión, etc.	

Fuente: (Crespo, 2016)

Tabla 21:
Alteración accidental de la información.

[NO_INTENCIONADO.6] Alteración accidental de la información	
Activos afectados: [IE] Información electrónica, [IP] Información en papel, [SW] Software, [EXTRAIBLE] Soportes de información, [ED] Edificaciones	**Dimensiones:** 1. [I] Integridad
Descripción: esta amenaza sólo se identifica sobre los datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

Fuente: (Crespo, 2016)

Tabla 22:
Destrucción de información.

[NO_INTENCIONADO.7] Destrucción de información	
Activos afectados: [IE] Información electrónica, [IP] Información en papel, [SW] Software, [EXTRAIBLE] Soportes de información, [ED] Edificaciones	**Dimensiones:** 1. [D] Disponibilidad

Descripción: esta amenaza hace referencia sobre la pérdida accidental de información, sólo se identifica sobre los datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

Fuente: (Crespo, 2016)

[EL] Errores lógicos

Ecu@Risk considera errores lógicos a las amenazas que afectan al software e información electrónica, se puede dar por diversos factores como: virus, programas mal compilados, etc.

Tabla 23:
Errores lógicos.

[EL.1] Difusión de software dañino	
Activos afectados: [SW] Software, [IE] Información electrónica	**Dimensiones:** 1. [D] Disponibilidad, 2. [I] Integridad, 3. [C] Confidencialidad
Descripción: propagación inocente de virus, spyware, gusanos, troyanos, bombas lógicas, malware en general.	

Fuente: (Crespo, 2016)

Tabla 24:
Copia no controlada de información.

[EL.2] Copia no controlada de información	
Activos afectados: [SW] Software, [IE] Información electrónica	**Dimensiones:** 1. [C] Confidencialidad
Descripción: la información es copiada accidentalmente sin fines maliciosos y sin el consentimiento del propietario.	

Fuente: (Crespo, 2016)

Tabla 25:
Escapes de información.

[EL.3] Escapes de información	
Activos afectados: Todos los activos	**Dimensiones:** 1. [C] Confidencialidad
Descripción: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en si misma sea alterada.	

Fuente: (Crespo, 2016)

[EC] Errores de Comunicaciones

Tabla 26:
Errores de [re-]encaminamiento.

[EC.1] Errores de [re-]encaminamiento	
Activos afectados: [SW] Software, [IC] Infraestructura de comunicaciones	**Dimensiones:** 1. [C] Confidencialidad
Descripción: envío de información a través de un sistema o una red usando accidentalmente una ruta incorrecta que lleve la información a donde o por donde no se debía; pudiendo tratarse mensajes entre personas, procesos, sistemas. Es particularmente destacable el caso de que el error de encaminamiento o ruteo suponga un error de entrega, acabando la información en manos de quién no se espera.	

Fuente: (Crespo, 2016)

Tabla 27:
Errores de secuencia.

[EC.2] Errores de secuencia	
Activos afectados: [SW] Software, [IC] Infraestructura de comunicaciones	**Dimensiones:** 1. [I] Integridad
Descripción: alteración accidental del orden de los mensajes transmitidos.	

Fuente: (Crespo, 2016)

2.3.3. Análisis de los riesgos

Una vez realizada la identificación de los riesgos y amenazas a la organización, se debe considerar las fortalezas y debilidades de los sistemas y procesos que hayan sido designados para controlar o mitigar los riesgos encontrados. Se debe conocer y evaluar los controles ya identificados e implementados, se debe analizar su eficiencia, es decir si contribuyen a la identificación de algo, o simplemente no colabora con ninguna acción.

Se define el procedimiento para realizar el análisis de los riesgos.

2.3.3.1. Identificar los controles existentes

Identificar los controles que ya están para mitigar el riesgo. Una vez identificados los controles, Ecu@Risk realiza una evaluación probabilística de que ocurra un riesgo y las consecuencias que conlleva la materialización del riesgo.

2.3.3.2. Evaluar la probabilidad

La metodología recomienda que la probabilidad del riesgo sea clasificada en cinco niveles, como se lo indica en la siguiente tabla.

Tabla 28:
Matriz de probabilidad.

Matriz de probabilidad	Número de incidentes similares producidos en los últimos 3 años	Probabilidad (%)	Calificación
E - Casi certero	11 en adelante	85-100	5
A - Aceptable	07 - 10	70 - 84	4
M - Posible	04 - 06	30 - 69	3
B - Baja no muy común	02 - 03	4 -29	2
L - Raro	1	1 - 3	1

Fuente: (Crespo, 2016)

2.3.3. Evaluar la consecuencia

La evaluación de las consecuencias es muy subjetiva, sin embargo, se recomienda sacar los datos de auditorías, inspecciones, información recogida, conocimiento laboral, etc.

La metodología recomienda evaluar las consecuencias mediante la siguiente tabla de riesgo – impacto.

Tabla 29:
Matriz de impacto.

Matriz de impacto	Valoración obtenida en Disponible, Integridad, Confidencialidad	Calificación
E - Extremo	9-10	5
A - Alto	6-8	4
M - Moderado	3-5	3
B - Menor	1-2	2
L - Leve	0	1

Fuente: (Crespo, 2016)

2.3.3.4. Valorar el riesgo

Para la valoración del riesgo la Ecu@Risk otorga una matriz de riesgo, la misma que permitirá evaluar los niveles de consecuencia y probabilidad. Crespo (2016) establece el cálculo del riesgo con la siguiente operación:

Riesgo= Probabilidad (calificación) x Impacto (calificación)

Luego de realizada la operación del cálculo del riesgo, los valores que puede recibir la Matriz de riesgos se clasifican en.

Tabla 30:
Matriz de valoración del riesgo.

Clasificación	Valoración	Calificación
E - Casi certero (frecuente)	20 -25	5
A - Probable	10 - 16	4
M - Posible	5 - 9	3
B - Baja o no muy común	2 - 4	2
L - Raro	1 - 2	1

Fuente: (Crespo, 2016)

Matriz de riesgos

Esta matriz es la representación gráfica de la multiplicación de la probabilidad que presente el riesgo por el impacto en el activo de información. El resultado de la operación, representa la valoración del riesgo, cuya clasificación es presenta en la Tabla 30.

Tabla 31:
Matriz de valoración del riesgo.

Matriz de Riesgos						
		Impacto				
		1. Leve	2. Menor	3. Moderado	4. Alto	5.Extremo
Probabilidad	E - Casi certero (frecuente)	M	M	A	E	E
	A - Probable	B	M	A	A	E
	M - Posible	B	M	M	A	A
	B - No muy común	B	B	M	M	A
	L - Raro	L	L	B	B	M

Fuente: (Crespo, 2016)

Ejemplo:

Se registra el sistema operativo de un servidor, su codificación sería [SW][STD][OS][01], tiene una calificación de Confidencialidad (C): 5, Disponibilidad (D): 7, Integridad (I): 7.

Primero se la analiza en la matriz de impacto, tanto la Confidencialidad, Disponibilidad e Integridad.

Disponibilidad

Matriz de impacto	Valoración obtenida en Disponibilidad	Calificación
E - Extremo	9-10	5
A - Alto	6-8	4
M - Moderado	3-5	3
B - Menor	1-2	2
L - Leve	0	1

Confidencialidad

Matriz de impacto	Valoración obtenida en Confidencialidad	Calificación
E - Extremo	9-10	5
A - Alto	6-8	4
M - Moderado	3-5	3
B - Menor	1-2	2
L - Leve	0	1

Integridad

Matriz de impacto	Valoración obtenida en Integridad	Calificación
E - Extremo	9-10	5
A - Alto	6-8	4
M - Moderado	3-5	3
B - Menor	1-2	2
L - Leve	0	1

Según registros un virus de secuestro (ransomware) ha atacado la red 4 veces en los últimos dos años. Con estos datos en la matriz de probabilidades se debe identificar su calificación.

Matriz de probabilidad	Número de incidentes similares producidos en los últimos 3 años	Probabilidad (%)	Calificación
E - Casi certero	11 en adelante	85-100	5
A - Aceptable	07 - 10	70 - 84	4
M - Posible	04 - 06	30 - 69	3
B - Baja no muy común	02 - 03	4 -29	2
L - Raro	1	1 - 3	1

El siguiente paso es realizar la operación de identificación del riesgo con los valores de probabilidad e impacto. (este ejemplo se lo realizará para la Disponibilidad del activo)

Riesgo= Probabilidad (calificación) x Impacto (calificación)

Riesgo= 3 x 3 = 9

Se compara el valor del riesgo con la tabla de valoración del riesgo.

Clasificación	Valoración	Calificación
E - Casi certero (frecuente)	20 -25	5
A - Probable	10 - 16	4
M - Posible	5 - 9	3
B - Baja o no muy común	2 - 4	2
L - Raro	1 - 2	1

El riesgo que se tiene en la Disponibilidad es “posible”. Finalmente, traduciendo el valor obtenido para la Matriz de Riesgos se tiene que:

Matriz de Riesgos						
		Impacto				
		1. Leve	2. Menor	3. Moderado	4. Alto	5.Extremo
Probabilidad	E - Casi certero (frecuente)	M	M	A	E	E
	A - Probable	B	M	A	A	E
	M - Posible	B	M	M	A	A
	B - No muy común	B	B	M	M	A
	L - Raro	L	L	B	B	M

Se debe repetir el mismo proceso para la Integridad y Confidencialidad.

2.3.4. Evaluación de los riesgos

El siguiente paso en la metodología es evaluar el riesgo, es decir, decidir de cuales son aceptables o inaceptables. Aceptar el riesgo significa que la organización va a disponerse a tolerar el mismo.

Según Crespo (2016) en una organización se puede tratar al riesgo como aceptable por diferentes circunstancias:

- No se dispone de tratamiento.
- Los costos del tratamiento son prohibitivos (particularmente relevante con referencia a riesgos de bajo impacto).
- El nivel de riesgo es bajo y no justifica el uso de los recursos.

Es importante aclarar que la relación que un riesgo sea aceptable o tolerable, no significa que sea insignificante, por lo tanto, un riesgo que sea considerado aceptable podría requerir ser supervisado.

Para evaluar el riesgo Crespo (2016) en su metodología propone la siguiente matriz para el registro y cálculo del riesgo.

Continuando con el ejemplo anterior, se tenía la amenaza de un virus de secuestro, que entra en la categoría de Difusión de software dañino [EL.1], y ya se han analizado todas sus dimensiones por lo que se utilizará la siguiente matriz.

	Valor					Impacto			Riesgo Acumulado			Riesgo absoluto	Contra-medida		Impacto			Riesgo residual		
Activo	C	D	I	TO-TAL	Frecuen-cia	C	D	I	C	D	I			Frecue-ncia	C	D	I	C	D	I
[SW][STD] [SO][01]	5	7	7	7																
[EL.1][1]					3	4	3	4	A	M	A	**A**								
Amenaza 2																				
Amenaza n																				

En los resultados se observa que en el campo “riesgo absoluto” el resultado es A, lo que significa que el riesgo [EL.1][1] es “Alto”, es el valor más alto de los indicadores del “riesgo acumulado”.

2.3.5. Tratamiento de los riesgos

La siguiente tabla representa los niveles de riesgo que se pueden presentar conjuntamente con las acciones de gestión requeridas de cada uno de los riesgos.

Tabla 32:
Niveles de riesgo.

Niveles de riesgo - Acción de gestión requerida	
Riesgo Extremo (E)	Requiere respuesta y atención inmediata.
Riesgo Alto (A)	Debe otorgársele la atención apropiada.
Riesgo Medio (M)	Evaluar el riesgo y determinar si los controles implementados son suficientes y si están efectivos.
Riesgo Bajo (B)	Administrar mediante procedimientos rutinarios; informar a los gestores locales; supervisar y revisar localmente como sea necesario.
Riesgo Leve (L)	Monitoreo constante a las actividades diarias. Registrar eventos en bitácora.

Fuente: (Crespo, 2016)

Según sea el cálculo del riesgo la organización debe seguir una serie de pasos que detalla la guía Ecu@Risk desarrollada por Crespo (2016), en donde se debe decidir qué riesgos serán tratados, con qué recursos, etc. Es decir, elaborar un plan de tratamiento de riesgos, donde se asignarán roles, responsabilidades, cronogramas de implementación para contrarrestar el riesgo, etc.

Se debe aplicar el plan de tratamiento en los riesgos como se haya establecido por la organización, realizar controles y documentar los detalles que tenga las aplicaciones de las medidas.

La metodología sugiere los siguientes pasos:

Paso 1

Una vez identificado el riesgo es necesario decidir si es necesario implementar un tratamiento específico o si se puede ser tratado durante el curso de procedimientos normalizados de gestión de actividades de la empresa, es decir integrar tratamientos o procedimientos en las prácticas del día a día que se realiza normalmente en la organización.

Paso 2

Se determina cuál es el objetivo del tratamiento del riesgo, es decir, se especifica si dicho riesgo se requiere reducirlo, transferirlo o simplemente aceptar el nivel de riesgo existente.

Paso 3

Se debe identificar y diseñar alguna opción para tratar el riesgo, una vez definido el objetivo en el paso anterior. Se debe considerar lo siguiente:

- Si el objetivo es reducir la probabilidad del riesgo, entonces debe considerar las causas de la amenaza y su relación causal con el impacto, ambos deben estar identificados en la fase de evaluación de riesgos.
- Comprender la naturaleza del riesgo y cómo se produce, proporciona una gran ventaja al momento de identificar de forma más sencilla las acciones que se deben tomar para mitigar el riesgo.
- Si el objetivo es reducir el impacto o consecuencia del riesgo, se deben elaborar planes de contingencia para responder a la materialización del riesgo.
- Si el objetivo es compartir el riesgo, entonces se requiere la participación de un tercero, tal como una aseguradora o un contratista. El compartir el riesgo no libera de obligaciones, ni evita asumir las consecuencias del daño.
- Si el objetivo es eliminar o evitar por completo el riesgo entonces las alternativas se limitan a cambiar el proyecto materialmente, elegir enfoques o procesos alternativos para convertir al riesgo en irrelevante o terminar en el abandono de la actividad programa. Se debe considerar que, en general, el riesgo no puede ser eliminado por completo y realizar un equilibrio es una parte importante en el ejercicio de aseguramiento de los mismos.
- En ocasiones la decisión de aceptar o tolerar el riesgo se debe a la baja probabilidad o impacto que representa a materialización de ese riesgo, otro motivo es que el costo de

controlarlo es injustificadamente alto, o que la oportunidad sea superior al riesgo. Estas decisiones deben documentarse cuidadosamente, de esta manera queden como referencias o evidencias.

Paso 4

Se debe evaluar las opciones de tratamiento y su viabilidad en relación con la tolerancia al riesgo. Es decir, cuestionarse si los controles seleccionados van a reducir o mitigar los riesgos en los cuales se los va a aplicar.

Paso 5

El siguiente paso es la documentación del plan de tratamiento del riesgo. Este plan deberá identificar roles, responsabilidades, definir cronograma para su implementación, presupuesto, indicadores de desempeño y revisión de procesos que fuesen apropiados.

Paso 6

Aplicar tratamientos acordados, una vez que todas las actividades hayan sido aprobadas y financiadas se procede a implementar el plan de tratamiento de riesgos y deben ser aplicados por las personas responsables que se hayan definido.

Paso 7

Se debe evaluar el riesgo residual que tiene el riesgo después de la implementación de los tratamientos, el riesgo residual se refiere a la probabilidad y la consecuencia de que el riesgo ocurra después de que el mismo haya sido tratado.

Para calcular el riesgo residual, se repite el procedimiento del cálculo de riesgo absoluto, sin embargo, ahora se considera una nueva frecuencia con la que se hayan presentado los incidentes. El riesgo residual no puede ser medido de inmediato (dependiendo del control) por lo que se sugiere la evaluación luego de un semestre.

Por lo general la calificación del riesgo residual después de ser implementado un tratamiento para un riesgo es inferior al valor nominal del riesgo, si pasa lo contrario significa que los controles implementados no son eficaces.

La siguiente tabla proporciona un resumen del tratamiento de riesgos:

Tratamiento de riesgo				
Riesgo identificado	**Tipo de tratamiento**	**Objetivo del tratamiento del riesgo mencionado**	**Origen del riesgo (Posibles causas)**	**Qué busca el control**

Fuente: (Crespo, 2016)

El registro de la contramedida se lo realizará dentro del plan de tratamiento del riesgo mediante la matriz indicada en la tabla 34.

Tabla 33:
Plan de tratamiento de riesgo.

Plan de tratamiento de riesgo									
Contramedida	Presupuesto	Inversión	Actividades	Responsables	Cronograma				
					SEM1	SEM2	SEM3	SEM4	SEM5
Contramedida	$	$	Actividad 1	Responsables					
			Actividad 2	Responsables					
			Actividad 3	Responsables					
			Actividad 4	Responsables					
			Actividad n	Responsables					

Fuente: (Crespo,2016)

2.3.6. Identificación de contramedidas

La metodología Ecu@Risk sugiere que para seleccionar las contramedidas que protegerán a los activos de información, se debe considerar, los elementos de protección actuales que se encuentran implementados en las organizaciones, y luego los posibles elementos de control que se podrían implementar. En base a los estudios realizados por Crespo (2016) en su metodología se sugieren controles que son aplicables al contexto de las capacidades que presentan una organización MPYME.

Tabla 34:
Plan de tratamiento de riesgo.

Tipo de protección	
PGeneral	Protección de tipo general.

PInfo	Protección de Información Electrónica y de Papel.
PSW	Protección de software.
PIC	Protección de la Infraestructura de Comunicaciones.
PSF	Seguridad Física, relativa a edificaciones e instalaciones.
PRRHH	Relativas a Recursos Humanos.

Fuente: (Crespo,2016)

Protección general

La metodología Ecu@Risk sugiere que al menos los siguientes elementos sean considerados en las protecciones de tipo general:

- Protección de acceso a lugares públicos.
- Cámaras de monitoreo.
- Extintores contra incendios.
- Sensores de humedad, calor, humo.
- Aspersores.
- Antivirus.
- Antispyware.
- Procedimiento para la gestión de vulnerabilidades.
- Segregación de tareas.
- Herramientas para la identificación y autenticación.
- Herramientas para monitorización de tráfico.
- Herramientas para el análisis de logs.
- Herramientas para el análisis de actualizaciones y parches de sistemas operativos.
- Defensa en profundidad.
- Procedimientos para aseguramiento de la disponibilidad.

Protección de información electrónica y de papel

La metodología Ecu@Risk sugiere que al menos los siguientes elementos sean considerados en la protección de información electrónica y de papel:

- Copias de seguridad de los datos.
- Cifrado de información sensible.
- Procedimientos para aseguramiento de la calidad.

- Gestión de llaves y certificados digitales.

Protección de software

La metodología Ecu@Risk sugiere que al menos los siguientes elementos sean considerados en la protección de software:

- Copias de seguridad.
- Procedimientos para puesta en producción.
- Procedimientos para modificación de software.
- Procedimientos para baja segura de software.

Protección de hardware

La metodología Ecu@Risk sugiere que al menos los siguientes elementos sean considerados en la protección de hardware:

- Protección de hardware (en ambientes de desarrollo, pre producción y producción).
- Procedimientos para la gestión de la disponibilidad.
- Procedimientos para la correcta operación.
- Procedimientos para la baja / reemplazo.
- Procedimientos para el manejo seguro de computación móvil.

Protección de la infraestructura de comunicaciones

La metodología Ecu@Risk sugiere que al menos los siguientes elementos sean considerados en la protección de la infraestructura de comunicaciones:

- Aseguramiento de la disponibilidad.
- Procedimiento para cambios (actualizaciones y mantenimiento).
- Consideraciones para el uso de internet.
- Consideraciones para el uso de telefonía móvil.
- Aseguramiento del canal.
- Aseguramiento de la entrada de servicio.

Seguridad física, relativa a edificaciones e instalaciones

La metodología Ecu@Risk sugiere que al menos los siguientes elementos sean considerados en la seguridad física, relativa a edificaciones e instalaciones:

- Protección de acceso a lugares sensibles.
- Cámaras de monitoreo y vigilancia.
- Extintores contra incendio.
- Sensores de humedad, calor, humo.
- Aspersores.
- Políticas de uso de infraestructura.
- Políticas ante emergencias.

Relativas a los recursos humanos

La metodología Ecu@Risk sugiere que al menos los siguientes elementos sean considerados en la protección relativa a los recursos humanos:

- Gestión del personal.
- Formación y concienciación.
- Aseguramiento de la disponibilidad.

Los elementos presentados en esta sección deben considerarse al momento de registrar contramedidas ante los riesgos identificados y registrados anteriormente.

2.4. Recursos

En este apartado se presentarán todas herramientas para la correcta utilización y documentación de la metodología Ecu@Risk.

Matrices para la identificación de activos de información

Las columnas C, D, I, hacen referencia a la Confidencialidad, Disponibilidad e Integridad, respectivamente.

Hardware

Tabla 35:
Matriz de identificación de activos de información. Hardware.

id_Activo	Incremental	Tipo	Número Serie	Mac	Fecha compra	Proveedor	Garantía	C	D	I	Valoración

Fuente: (Crespo, 2016)

Software

Tabla 36:
Matriz de identificación de activos de información. Software.

id_Activo	Incre-mental	Descrip-ción	Ver-sión	Número de serie	Clave de activación	Fecha compra	Actuali-zación	Provee-dor	C	D	I	Valora-ción

Fuente: (Crespo, 2016)

Información electrónica

Tabla 37:
Matriz de identificación de activos de información. Información electrónica.

id_ Activo	Incre-mental	Tipo	Fecha creación	Ta-maño	Permi-sos	Ubica-ción	Nom-bre	Fecha modificación	Crea-dor	C	D	I	Valora-ción

Fuente: (Crespo, 2016)

Información Papel

Tabla 38:
Matriz de identificación de activos de información. Información en papel.

id_Activo	Incremental	Tipo	Fecha creación	Ubicación	Nombre	Fecha modificación	Creador	C	D	I	Valor-ación

Fuente: (Crespo, 2016)

Infraestructura de comunicaciones

Tabla 39:
Matriz de identificación de activos de información. Infraestructura de comunicaciones.

id_Activo	Incremental	Tipo	Categoría	Nombre	Proveedor	Fecha contrato	C	D	I	Valoración

Fuente: (Crespo, 2016)

Medios de almacenamiento extraíbles

Tabla 40:
Matriz de identificación de activos de información. Medios de almacenamiento extraíbles.

id_Activo	Incremental	Tipo	Categoría	Mac	Fecha adquisición	Proveedor	Garantía	C	D	I	Valoración

Fuente (Crespo, 2016)

Recursos humanos

Tabla 41:
Matriz de identificación de activos de información. Recursos humanos.

id_Activo	Incremental	Nombre	Apellido	Cargo	Género	Fecha de ingreso	Fecha de salida	C	D	I	Valoración

Fuente: (Crespo, 2016)

Edificaciones / Instalaciones

Tabla 42:
Matriz de identificación de activos de información. Edificaciones / Instalaciones.

id_Activo	Incremental	Descripción	Ubicación	C	D	I	Valoración

Fuente: (Crespo, 2016)

Matriz para el registro de riesgos

Tabla 43:
Matriz para el registro de riesgos.

[COD RIESGO] RIESGO	
Activos afectados:	**Dimensiones:** [D] Disponibilidad [I] Integridad [C] Confidencialidad
Descripción:	

Fuente: (Crespo, 2016)

Registro y cálculo de riesgos

Tabla 44:
Matriz para registro el cálculo de riesgos.

	Valor					Impacto			Riesgo Acumulado			Riesgo absoluto	Contra-medida		Impacto			Riesgo residual		
Activo	C	D	I	TO-TAL	Frecuen-cia	C	D	I	C	D	I			Frecue-ncia	C	D	I	C	D	I

Fuente: (Crespo, 2016)

Matriz para el manejo de riesgos

Tabla 45:
Matriz para el manejo de riesgos.

Matriz de Riesgos						
		Consecuencia				
		1. Leve	2. Menor	3. Moderado	4. Alto	5.Extremo
Probabilidad	E - Casi certero (frecuente)	M	M	A	E	E
	A - Probable	B	M	A	A	E
	M - Posible	B	M	M	A	A
	B - No muy común	B	B	M	M	A
	L - Raro	L	L	B	B	M

Fuente: (Crespo, 2016)

Tabla 46:
Niveles de riesgo.

Niveles de riesgo - Acción de gestión requerida	
Riesgo Extremo (E)	Requiere respuesta y atención inmediata.
Riesgo Alto (A)	Debe otorgársele la atención apropiada.
Riesgo Medio (M)	Evaluar el riesgo y determinar si los controles implementados son suficientes y si están efectivos.
Riesgo Bajo (B)	Administrar mediante procedimientos rutinarios; informar a los gestores locales; supervisar y revisar localmente como sea necesario.

Riesgo Leve (L)	Monitoreo constante a las actividades diarias. Registrar eventos en bitácora.

Fuente: (Crespo, 2016)

Matriz para el tratamiento de riesgos

Tabla 47:
Tratamiento de riesgos.

Tratamiento de riesgo				
Riesgo identificado	**Tipo de tratamiento**	**Objetivo del tratamiento del riesgo mencionado**	**Origen del riesgo (Posibles causas)**	**Qué busca el control**

Fuente: (Crespo, 2016)

Matriz para el plan de tratamiento de riesgos

Tabla 48:
Plan de tratamiento de riesgos.

Plan de tratamiento de riesgo									
Contramedida	Presupuesto	Inversión	Actividades	Responsables	Cronograma				
					SEM1	SEM2	SEM3	SEM4	SEM5
Contramedida	$	$	Actividad 1	Responsables					
			Actividad 2	Responsables					
			Actividad 3	Responsables					

Fuente: (Crespo, 2016)

2.5. Conclusiones capítulo 2

La metodología propone claramente a los actores y define los roles de participación de cada uno dentro de la gestión de riesgos, cabe recalcar que cada rol es importe ya que contribuye a que el marco de gestión de riesgo de la metodología sea efectivo. Se busca la participación activa de todos los sectores que conforman la empresa, tales como: el gobierno institucional, la planeación y estrategias, para que juntos trabajen en la identificación, planificación, tratamiento y mitigación de los riesgos.

La gestión de riesgo que aplica la metodología Ecu@Risk se basa en el modelo de Deming; i) se planifica cómo se van a tratar a los riesgos, asignando recursos y definiendo objetivos, ii) se ejecuta la planificación, es decir, se implementan los tratamientos definidos anteriormente

en la primera etapa, iii) se verifica si los tratamientos de los riesgos han sido eficaces o no han cumplido los objetivos planteados, iv) si es necesario corregir problemas en los tratamientos se debe actuar para solucionar, el modelo de Deming es cíclico, es decir siempre estará en constante aplicación y redundancia en cada una de sus etapas con todos los tratamientos y aspectos de la metodología Ecu@Risk.

Ecu@Risk propone categorías y subcategorías para el registro de activos de información de las empresas, además propone medidas de valoración, los cuales indican la importancia del activo para el negocio y sus procesos, la valoración se lo realiza en dimensiones de: disponibilidad, integridad y confidencialidad. La metodología es muy clara en la manera de identificar y registrar los activos de cada empresa, por lo que no representaría mayor inconveniente realizar el inventario de los mismos.

Los riesgos derivan de las categorías de amenazas establecidas por la metodología Ecu@Risk, una vez, identificado y registrado el riesgo se lo valoriza, a partir de la probabilidad en que se pueda llegar a materializar dicho riesgo. Para el cálculo de riesgo residual la metodología utiliza la fórmula Impacto x Probabilidad, la cual da la valoración que representa el riesgo para el activo de información, y los miembros de la empresa deben decidir qué hacer con el mismo.

Para el establecimiento de contramedidas Ecu@Risk establece el desarrollo de planes de tratamiento de riesgo, en el cual se especifica qué se desea lograr con el riesgo; la implementación y posterior evaluación de la contramedida da como resultado el riesgo residual que representa el nivel actual en que afecta el riesgo al activo de información, con esta información se decide si el plan de tratamiento es eficiente o no, si no lo es el ciclo de Deming de la metodología vuelve a empezar.

La metodología Ecu@Risk presenta una gestión muy entendible y adaptable a las empresas MPYMES, cubriendo todos los aspectos más importantes de la gestión de riesgos establecidas por normas y metodologías internacionales, lo que lo hace aplicable y viable en el entorno en el cual se desarrollan las empresas. La aplicación de la metodología promoverá el desarrollo de la conciencia y cultura de seguridad de información a en todas las empresas.

Capítulo 3: Análisis comparativo de software para la gestión de riesgos y levantamiento de requerimientos

Análisis comparativo de software para la gestión de riesgos

3.1. Introducción

Este capítulo comprende el análisis de diferentes herramientas para la gestión de riesgos, aplicando el estándar internacional ISO/IEC 9126 para la evaluación de la calidad del software, ya que es un modelo que puede aplicarse a cualquier producto software. (Muhairat, Alrawashdeh, & Althunibat , 2013)

Lo que se busca en esta evaluación es obtener un modelo base para la construcción del software de la metodología Ecu@Risk.

3.2. ISO/IEC 9126

Según la autora Cochea (2009), el estándar ISO/IEC 9126 está orientado a dos áreas de la calidad:

- Calidad interna y externa.
- Calidad en uso del producto software.

Para el análisis comparativo que se plantea hacer se tomará en cuenta un área del estándar, que es la calidad interna y externa. Coshea (2009) indica que esta área se divide en las siguientes características y subcaracterísticas.

- Funcionalidad.
    - Adecuación.
    - Exactitud.
    - Interoperabilidad.
    - Seguridad.
- Fiabilidad.
    - Madurez.
    - Recuperabilidad.
    - Tolerancia a fallos.
- Usabilidad.

  - Aprendizaje.
  - Comprensión.
  - Operatividad.
  - Atractividad.

- Eficiencia.
  - Comportamiento en el tiempo.
  - Comportamiento de recursos.

- Mantenibilidad.
  - Estabilidad.
  - Facilidad de análisis.
  - Facilidad de cambios.
  - Facilidad de pruebas.

- Portabilidad
  - Capacidad de instalación.
  - Capacidad de reemplazamiento.
  - Adaptabilidad.
  - Co-existencia.

Los autores Largo García & Marín Mazo (2005) en su guía para evaluación de software presentan los conceptos de cada uno de las características y subcaracterísticas del área del estándar de la ISO/IEC 9126 elegido para realizar el análisis.

3.2.1. Funcionalidad

Hace referencia a la capacidad del software de realizar las funciones para cumplir las necesidades (explícitas o implícitas) cuando es usado bajo ciertas condiciones, es decir, se evalúa la capacidad del software de cumplir las necesidades para las cuales fue requerido.

Adecuación: es la capacidad del software para proporcionar un conjunto de funciones que realicen las tareas y que cumplan los objetivos que hayan sido especificados por el usuario.

Exactitud: se refiere a la capacidad del software para realizar tareas y obtener resultados de forma precisa o de la forma que sea esperada.

Interoperabilidad: es la capacidad del software para relacionarse e interactuar con uno o más sistemas específicos.

Seguridad: es la capacidad del software de acceder a los datos de los usuarios o sistemas autorizados a aquellos usuarios que sean autorizados, es decir, es la capacidad de software de proteger los datos para que ningún usuario o sistema autorizado pueda modificarlos o hacer operaciones con ellos.

3.2.2. Confiabilidad

Se refiere a la capacidad del software para garantizar su funcionamiento adecuado bajo ciertas circunstancias específicas.

Madurez: capacidad que mantiene el software para evitar fallas a pesar de que ocurra algún error.

Tolerancia a fallos: es la capacidad del software para continuar un correcto funcionamiento en caso de que ocurra algún error.

Recuperabilidad: es la capacidad del software para volver a su funcionamiento normal y recuperar los datos afectados cuando ocurra una falla o error.

3.2.3. Usabilidad

Es la capacidad del software de ser aprendido, comprendido y usado de manera fácil y atractiva; esta característica es evaluada por los usuarios finales e indirectos.

Aprendizaje: la manera en que el software permite su el aprendizaje de su uso a los usuarios.

Comprensión: es la capacidad del software que permite al usuario entender el cómo ser utilizado en las tareas y cuáles son las condiciones de uso.

Operatividad: es la forma como el software permite al usuario controlarlo y operarlo.

Atractividad: se refiere a la presentación del software (interfaz gráfica) hacia el usuario.

3.2.4. Eficiencia

Se refiere al desempeño del software, de acuerdo al número de recursos utilizados según las condiciones dadas.

Comportamiento en el tiempo: el tiempo de respuesta al procesamiento de una función de software bajo condiciones específicas.

Comportamiento de recursos: la utilización de cantidades y tipos adecuados de recursos cuando el software funcione bajo requerimientos o condiciones dadas.

3.2.5. Mantenibilidad

Se define como la capacidad que tiene el software para ser modificado, esto incluye correcciones o mejoras del mismo.

Estabilidad: es la capacidad del software para evitar eventos imprevistos para modificaciones del mismo.

Facilidad de análisis: se refiere a la forma como el software permite analizar y diagnosticar deficiencias o fallas, así también como las partes modificadas del software.

Facilidad de cambio: se refiere a la capacidad del software para que se pueda poner en funcionamiento una modificación.

Facilidad de pruebas: es la facilidad con la que se puede realizar pruebas de una modificación realizada, sin poner en riesgo a los datos del software.

3.2.6. Portabilidad

Se refiere a la capacidad del software de ser trasladado de un entorno a otro, sin alterarlo de ninguna manera.

Capacidad de instalación: es la facilidad con la que el software puede ser instalado en un entorno específico.

Capacidad de reemplazamiento: es la capacidad que tiene el software para ser reemplazado por otro del mismo tipo, que cumpla con las mismas funciones y persiga el mismo objetivo.

Adaptabilidad: es la capacidad del software para adaptarse a diferentes entornos, sin que exista una reacción negativa frente a cualquier cambio.

Co-existencia: es la capacidad que posee el software para estar en el mismo ambiente que otros softwares, también la manera en que comparten recursos con los mismos.

Una vez conocidos los conceptos de las características y subcaracterísticas del área de calidad interna y externa del estándar ISO/IEC 9126 presentados por Largo García & Marín Mazo (2005), se puede definir qué se evaluará de cada software para la gestión de riesgos que se plantea en este capítulo.

Para la elaboración de la guía de evaluación de las herramientas de software para la gestión de riesgos se toma en consideración el funcionamiento de la metodología Ecua@Risk, la cual se enfoca en la gestión de activos y riesgos de información.

3.3. Guía de evaluación

A continuación, se describirá la guía de evaluación con todas las características y subcaracterísticas escogidas para ser analizadas en los diferentes softwares de gestión de riesgos de información.

Funcionalidad

Dentro de la característica de la funcionalidad para la evaluación se ha tomado en cuenta las siguientes subcaracterísticas:

Adecuación: para esta subcaracterística lo que se plantea evaluar es que el software cumpla con la gestión de activos de información, gestión de amenazas, gestión de contramedidas, análisis de riesgos y generación de informes.

La gestión de activos de información quiere decir, que exista la posibilidad de registrar activos de información, así como también la posibilidad de valorarlos, en dimensiones de disponibilidad, integridad y confidencialidad. Dentro del registro de activos de información se plantea que el software contemple categorías establecidas como: edificaciones, hardware, software, información electrónica, información en papel, medios de almacenamiento extraíble, infraestructura de comunicaciones y recursos humanos. En cada categoría se evalúa también las subcategorías descritas dentro de la metodología Ecu@Risk.

La gestión de amenazas analiza la posibilidad de que se pueda registrar una amenaza, la misma que puede ser una de las siguientes categorías: riesgo natural, riesgo provocado (deliberado), riesgo provocado (por error), riesgo informático, riesgo comunicacional y otros. Se analiza que la amenaza pueda ser valorada, en dimensiones de disponibilidad, integridad y confidencialidad.

La gestión de contramedidas analiza la posibilidad de que se pueda registrar una contramedida, la misma que puede pertenecer a una de las siguientes categorías: protección general, protección de información electrónica y en papel, protección de software, protección de hardware, protección de infraestructura de comunicaciones, protección física, relativa a edificaciones e instalaciones, protección relativa a recursos humanos y otros. Así mismo, se analiza la posibilidad que la contramedida pueda ser valorada en dimensiones de disponibilidad, integridad y confidencialidad.

En análisis de riesgos, se requiere que exista la posibilidad de registrar la probabilidad de que la amenaza registrada se materialice, así mismo, se requiere que exista una evaluación de la consecuencia, es decir, una valoración de la consecuencia si la amenaza se llegara a materializar. Se requiere valorar el riesgo mediante la multiplicación de la probabilidad y la consecuencia registrados anteriormente. Se evalúa que el software tenga el cálculo del riesgo absoluto y riesgo residual, mismos que ya fueron explicados en el análisis de la metodología Ecu@Risk.

Se evalúa que el software genere informes de análisis de los riesgos registrados, e informes de activos de información con respecto a los riesgos. Si existe otro tipo de informes serán registrados en el informe de evaluación.

Exactitud: en esta subcategoría se enfoca en verificar que los resultados presentados del cálculo de los riesgos (absoluto y residual) sean preciosos, es decir que exista un error de 0% en el cálculo realizado por el software.

Interoperabilidad: en esta subcategoría se evaluará la interoperabilidad de archivos, es decir, qué tipos de archivos se van a poder importar o exportar del software en análisis, a partir de esos archivos generados se va a poder utilizar esa información en otras herramientas.

Seguridad: dentro de esta subcategoría se plantea evaluar que el software cuente con diferentes usuarios con sus respectivos permisos para poder modificar y visualizar la información, así como que se tenga un registro de actividad para conocer qué usuario modificó algún dato. También como parte de medida de seguridad, se evaluará si se tiene acceso al código fuente de la aplicación, al igual que si se conoce la ubicación de los directorios generados por la aplicación, debido a que se puede prestar fácilmente a ataques cibernéticos.

Fiabilidad

En la característica de fiabilidad, serán evaluadas las siguientes subcaracterísticas:

Madurez: se plantea evaluar cómo ha ido evolucionando el software a través de los años, es decir cuántas versiones han sido lanzadas y cuántos años ha estado consolidado en el mercado dicho software, relacionado con una mejora del software ante las fallos detectados y corregidos en cada versión.

Tolerancia a fallos: lo que se busca evaluar en esta subcategoría es la capacidad que tiene el software a reportar los fallos en caso de que se produzca algún error y que no se altere de ninguna manera su funcionalidad.

Recuperabilidad: se analiza el comportamiento del software después de que exista alguna falla de algún tipo, se busca que los datos que no se hayan guardado antes de que se produzca la falla, puedan ser recuperados de alguna manera.

Usabilidad: en la categoría usabilidad, serán evaluadas las siguientes subcategorías:

Aprendizaje: en esta subcategoría se busca que el software tenga una diversidad de lenguajes para que sea más fácil su aprendizaje. Al igual que se evalúa que las herramientas del software sean fáciles de aprender y memorizar con nombres nemotécnicos.

Comprensión: se analiza la capacidad del software que tiene para utilizar elementos conocidos para los usuarios, como son los íconos que usualmente utilizan en casi todos los programas. Se plantea también analizar si el software brinda toda la información al usuario sobre el funcionamiento de cada herramienta, si se explica los resultados que va a obtener con el uso de las mismas, etc., todo con el fin de ayudar a la comprensión del software al usuario.

Operatividad: para la operatividad se evalúa el número de pasos que necesita el software para: registrar activos, registrar amenazas, registrar contramedidas, calcular el riesgo absoluto, calcular el riesgo residual y finalmente para generar informes.

Eficiencia

En la característica de eficiencia, será evaluada la siguiente subcaracterística:

Comportamiento de recursos: se requiere establecer los recursos necesarios tanto en hardware como en software para que el software pueda funcionar normalmente. Así mismo los porcentajes de ejecución tanto de memoria RAM, de uso de disco duro, y uso de CPU.

Mantenibilidad

En la característica de mantenibilidad, será evaluada la siguiente subcaracterística:

Facilidad de análisis: se plantea analizar si el software presenta documentación de desarrollo por medio de manuales de usuario, ventanas de ayuda, ayuda online, u otra forma en la que el usuario pueda analizar y pueda comparar los cambios realizados en el software, de modo que esto le pueda servir para aprender a usar la herramienta.

Portabilidad: en la última característica que se plantean evaluar las siguientes subcaracterísticas:

Capacidad de instalación: se evalúa la facilidad con la que se puede instalar el software y todos los recursos que se necesita para hacerlo en porcentaje de memoria RAM, uso de disco duro y uso de CPU.

Transportabilidad: en esta subcaracterística se evaluará en qué plataformas puede correr el software, es decir, qué sistemas operativos soportan su funcionamiento, puede ser Windows, Linux, Mac, etc.

3.4. Software de evaluación

Una vez definidos los parámetros para realizar el análisis, se escoge cuáles serán las herramientas para realizar el mismo. En este caso se escogieron 3 software para la gestión de riesgos de información: PILAR, SimpleRisk y Análisis de riesgos de INCIBE.

PILAR

La página web EAR/PILAR (sin fecha), define a Pilar como una herramienta que sirve para automatizar el análisis de riesgos de información. Se utiliza en el proceso de gestión de riesgos:

- Análisis inicial y regular de los riesgos.
- Medidas de control sobre riesgo residual.
- Diseño de planes de mejora de seguridad.

Es un software que usa la metodología Magerit, ha sido parcialmente financiado por el Centro Criptológico Nacional (CCN) de España, lanzado en el año 2004 ha ido evolucionando durante los años hasta la actualidad que se considera uno de los softwares de gestión de riesgos más estables.

El software es comercial, sin embargo, cuenta con una versión de prueba la cual puede ser utilizada sin licencia (muy pocas funciones) o con una licencia de prueba, la cual se tarda dos

semanas en llegar desde su petición, el software en su versión de prueba trabaja con archivos mrg en modo “read only”, para poder trabajar con una base de datos se requiere una licencia comercial. El precio del software varía de acuerdo a la versión, PILAR va desde los más básico que simplemente es el análisis de riesgos muy rápidos, hasta su versión completa para empresas. Los precios son los siguientes:

Tabla 49:
Precios del software Pilar.

Herramienta	Costo
μPILAR	250 €
PILAR Basic	500 €
PILAR Estándar	1.500 €
PILAR Estándar + BBDD	2.000 €
RMAT	3.000 €

Fuente: (EAR/PILAR, s.f.)

Para realizar el análisis del software se tomará la versión de PILAR estándar 6.2.6 con una licencia de prueba.

Simple Risk

Es una herramienta que es parte del Proyecto de seguridad de aplicaciones web abiertas, OWASP, por sus siglas en inglés, creada para la gestión de riesgos de información, su primera versión fue creada por Josh Sokol y lanzada en el año 2013. Esta herramienta fue pensada para que la administración del riesgo sea accesible para todos los profesionales de la seguridad y no solo para aquellos que puedan comprar una plataforma.

Se centra en la gestión de riesgos, utilizando varios métodos para la valoración de los mismos, como: CVS, OWASP DREAD, métodos clásicos para la valoración (basados en probabilidad e impacto) o también personalización de valorizaciones.

SimpleRisk ofrece diferentes versiones para los usuarios:

- SimpleRisk Core: esta es una versión gratis de código abierto, escrito en PHP con un back-end de base datos MySQL. El usuario se lo puede descargar, instalar, configurar y empezar a utilizarlo sin problema alguno.

- SimpleRisk Extra: permite añadir funcionalidades a la versión Core (gratuita), la licencia es anual y el precio depende de las características que se requiera adherir.
- SimpleRisk Hosted: es un servicio que ofrece la plataforma SimpleRisk de alojamiento desde sus propios servidores, depende de las necesidades del usuario cuenta con tres diferentes presentaciones: para individuos o pequeños equipos, para múltiples equipos dentro de una sola unidad de negocio, y finalmente para grandes empresas. Es una licencia anual de uso.

Tabla 50:
Precios del software SimpleRisk.

Herramienta	Costo		
SimpleRisk Core	0$		
SimpleRisk Extra	Basic	Plus	Premium
	9.995,00$	14.995,00$	19.995,00$
SimplerRisk Hosted	Small Enterprise	Medium Enterprise	Large Enterprise
	4.995,00$	9.995,00$	19.995,00$

Fuente: (SimpleRisk, 2017)

(SimpleRisk, 2017)

Para realizar el análisis del software se usará la versión Core de SimpleRisk v.20170724-001 instalada localmente en la máquina de prueba.

Análisis de riesgos de INCIBE

Es una herramienta creada para el análisis de riesgos que se presenta como ejercicio en el Plan de Director de Seguridad de INCIBE (Instituto Nacional de Ciberseguridad de España), cabe recalcar que no se presenta como un software en sí, más bien es una herramienta creada en Microsoft Excel, contando con funcionalidades muy básicas. Sin embargo, lo que resalta de la herramienta es que cubre lo básico en gestión de riesgos de activos de información, y nos hace ver, que cuando existe una conciencia de seguridad de la información, de cualquier manera, se lo busca implementar.

INCIBE publica los pasos para realizar un análisis de riesgos, es un análisis estándar que todas las metodologías de gestión de riegos lo aplican, dentro de la publicación se incluye la herramienta que será evaluada. La herramienta utiliza la metodología Magerit y dentro de ella

se explica paso a paso como registrar un activo de información, asociarlo a una amenaza para finalmente valorar dicho activo y obtener el resultado del riesgo final.

3.5. Evaluación

A continuación, se procederá con la evaluación y análisis de las tres herramientas descritas anteriormente, aplicando la guía de evaluación basada en la ISO/IEC 9126 propuesta anteriormente en este capítulo.

Todas las pruebas de las instalaciones de los programas de gestión de riesgos se realizaron en una computadora portátil Toshiba Satellite S55t-A5389, procesador Intel ® Core ™ i7-4700MQ CP @ 2.40GHz 2.40Ghz, Memoria RAM de 8GB y Disco duro de 750 GB.

Consideraciones de la evaluación

En esta evaluación la letra x representa que el atributo evaluado cumple (verdadero), y el espacio en blanco representa que el atributo evaluado no se cumple (falso).

Desarrollo

Software para el registro y evaluación de activos de información					
	Medición	Descripción	PILAR	Análisis de riesgos INCIBE	SimpleRisk
Funcionalidad	Función OBA	ISO/IEC 9126			
Adecuación	Función OBA	ISO/IEC 9126			
Gestión de activos de información	Función OBA	Atributos relacionados con la gestión de activos de información			
Registro de activos de información	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información	x	x	x
Edificaciones	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información de categoría Edificación	x	x	x
Centro principal de cómputo	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como centro de cómputo			
Centro de procesamiento alterno	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como centro de procesamiento alterno	x		
Espacio de atención a los clientes	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como espacio de atención a los clientes			

Área de contabilidad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como área de contabilidad			
Área sensible	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como área sensible			
Gerencia	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como gerencia			
Área financiera	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como área financiera			
Área de ventas	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como área de ventas			
Seguridad y vigilancia	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como seguridad y vigilancia			
Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como otros	x	x	x
Hardware	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información de categoría Hardware	x	x	x
Servidores	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como servidores	x		

Equipos de escritorio (PC)	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como equipos de escritorio (PC)	x		
Computadores portátiles (Laptops)	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como teléfonos celulares	x		
Teléfonos celulares	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como computadores portátiles (laptops)	x		
Impresoras	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como impresoras	x		
Escáneres	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como escáneres	x		
Impresoras multifuncionales	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como impresoras multifuncionales	x		
Sistema de transmisión de FAX	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como sistema de transmisión de FAX	x		
Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como otros	x	x	x
Software	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información de categoría Software	x	x	x

Desarrollo propio	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como software de desarrollo propio	x		
Desarrollo sub contratado	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como software de desarrollo subcontratado	x		
Software Estándar	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como software estándar	x		
Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como otros	x	x	x
Información electrónica	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información de categoría Información electrónica	x		
Archivos	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como archivos	x		
Archivos de respaldo	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como archivos de respaldo	x		
Archivos de configuración	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como archivos de configuración	x		

Archivos de contraseña	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como archivos de contraseña	x		
Archivos de registro de actividades	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como archivos de registro de actividades	x		
Tablas y base de datos	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como tablas y bases de datos	x		
Código ejecutable	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como código ejecutable	x		
Código fuente	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como código fuente	x		
Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como otros	x	x	x
Información en papel	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información de categoría Información en papel			
Documentos	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como documentos	x		
Copia del documento	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como copia del documento	x		

	Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como otros	x	x	x
Medios de almacenamiento extraíble		Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información de categoría Medios de almacenamiento extraíble			
	Óptico	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como medio de almacenamiento óptico	x		
	Electrónico	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como medio de almacenamiento electrónico	x		
	Mecánico	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como medio de almacenamiento mecánico	x		
	Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como otros	x	x	x
Infraestructura de comunicaciones		Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información de categoría Infraestructura de comunicaciones			
	Router	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como router	x		

Switch	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como switch	x		
Hub	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como hub	x		
Central telefónica	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como central telefónica	x		
Voz sobre IP	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como voz sobre IP	x		
Módem	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como módem	x		
Red Wifi	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como red wifi	x		
Red LAN	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como red LAN	x		
Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como otros	x	x	x
Recursos humanos	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información de categoría Recursos humanos	x		

	Usuario externo	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como usuario externo	x		
	Usuario interno	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como usuario interno	x		
	Personal de TI	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como personal de TI	x		
	Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar un activo de información como otros	x	x	x
Valoración de activos de información		Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar un activo de información	x		x
	Valoración de Disponibilidad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar la disponibilidad	x		x
	Valoración de Integridad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar la integridad	x		x
	Valoración de Confidencialidad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar la confidencialidad	x		x
	Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de otro tipo de valoración			

Gestión de amenazas	Función OBA	Atributos relacionados con la gestión de amenazas			
Registro de amenazas	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de identificar una amenaza	x	x	x
Riesgos naturales	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una amenaza de categoría de Riesgos naturales	x	x	x
Riesgos provocados (deliberados)	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una amenaza de categoría de Riesgos provocados (deliberados)	x	x	x
Riesgos provocados (por error)	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una amenaza de categoría de Riesgos provocados (por error)	x	x	x
Riesgos informáticos	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una amenaza de categoría de Riesgos informáticos	x	x	x
Riesgos comunicacionales	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una amenaza de categoría de Riesgos comunicacionales	x	x	x
Valoración de amenazas	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar una amenaza	x	x	x

Valoración de Disponibilidad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar la disponibilidad	x		x
Valoración de Integridad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar la integridad	x		x
Valoración de Confidencialidad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar la confidencialidad	x		x
Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de otro tipo de valoración		x	
Gestión de contramedidas	Función OBA	Atributos relacionados con la gestión de contramedidas			
Registro de contramedidas de contramedidas	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar contramedidas	x		x
Protección general	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una contramedida como protección general	x		

Protección de información electrónica y en papel	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una contramedida como protección de información electrónica y en papel	x		
Protección de hardware	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una contramedida como protección de hardware	x		
Protección de infraestructura de comunicaciones	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una contramedida como protección de infraestructura de comunicaciones	x		
Protección física, relativa a edificaciones e instalaciones	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una contramedida como protección física, relativa a edificaciones e instalaciones	x		
Protección relativa a Recursos humanos	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una contramedida como protección relativa a recursos humanos	x		
Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de registrar una contramedida como otros	x		x
Valoración de contramedidas	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar las contramedidas	x		x

Valoración de Disponibilidad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar la disponibilidad			
Valoración de Integridad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar la integridad			
Valoración de Confidencialidad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar la confidencialidad			
Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de otro tipo de valoración	x		x

Análisis de riesgos	Función OBA	Atributos relacionados con el análisis de riesgos			
Evaluación de probabilidad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de evaluación de probabilidad	x	x	x
Evaluación de consecuencia	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de evaluación de consecuencia	x	x	x
Cálculo de Riesgo absoluto	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de cálculo de riesgo absoluto	x	x	x
Cálculo de riesgo residual	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de cálculo de riesgo residual	x		
Valorar el riesgo	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de valorar el riesgo	x	x	x

Generación de informes	Función OBA	Atributos relacionados con la generación de informes			

Análisis de riesgos	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de generar informes de análisis de riesgos	x	x	x
Informe de amenazas	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de generar informes de amenazas	x	x	x
Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de generar otros informes	x		x

Exactitud	Función OBA	ISO/IEC 9126			
Herramientas de cálculo de riesgos	Función OBA	Atributos relacionados con las herramientas de cálculo de riesgos			
Cálculo de riesgo absoluto	Función: ((riesgo_calcuado:Float)-(riesgo_calculado_programa:Float)/(riesgo_calculado_programa:Float))*100 = Float	Diferencia porcentual entre el error calculado del riesgo	0%	0%	0%
Cálculo de riesgo residual	Función: ((riesgo_calcuado:Float)-(riesgo_calculado_programa:Float)/(riesgo_calculado_programa:Float))*100 = Float	Diferencia porcentual entre el error calculado del riesgo	0%	No calcula	No calcula

Interoperabilidad			Función OBA	ISO/IEC 9126			
	Interoperabilidad de archivos		Función OBA	Atributos relacionados a la interoperabilidad con archivos			
		Importar archivos	Función OBA	Atributos relacionados a la importación de archivos			
			Archivos tipo mgr	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de importar un archivo tipo mgr	x		
			Archivos tipo xml	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de importar un archivo tipo xml	x	x	
			Archivos tipo csv	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de importar un archivo tipo csv	x	x	x
			Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de importar otro tipo de archivo		x	
		Exportabilidad de archivos	Función OBA	Atributos relacionados a la exportación de archivos			
			Archivos tipo mgr	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de exportar un archivo tipo mgr	x		
			Archivos tipo xml	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de exportar un archivo tipo xml	x	x	
			Archivos tipo csv	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de exportar un archivo tipo csv	x	x	x
			Archivos tipo rtf	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de exportar un archivo tipo rtf	x		
			Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de exportar otro tipo de archivo		x	

Seguridad	Función OBA	ISO/IEC 9126			
Usuarios	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de tener diferentes tipos de usuarios			x
Permisos de usuarios	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de tener diferentes tipos de permisos de usuarios			x
Registros de actividad	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de tener registros de actividad de los usuarios			x
Acceso al código fuente	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de tener acceso al código fuente del programa			x
Ubicación de los directorios	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de obtener acceso a ubicación de los directorios	x	x	x

Fiabilidad	Función OBA	ISO/IEC 9126			
Madurez	Función OBA	ISO/IEC 9126			
Versiones	Función OBA	Atributos relacionados con las versiones del software			
Lista de versiones del producto	Versiones: Conjunto (Etiqueta, Nominal), Etiquetas:(1,1, 3,2,...)	Lista de versiones del software (ej.: 3.3, 5.2,..)	PILAR: 6.2.6 - 24.4.2017 PILAR: 6.2.5 - 15.3.2017 PILAR: 6.2.4 - 13.2.2017 PILAR: 6.2.3 - 10.1.2017 RMAT: 5.5.0 - 10.1.2017	Única versión.	SimpleRisk v.20170724-001 SimpleRisk v.20170723-001 SimpleRisk v.20170614-001 SimpleRisk v.20170416-001

			PILAR: 5.4.12 - 23.12.2016 PILAR: 6.2.2 - 19.12.2016 PILAR: 6.2.1 - 7.12.2016 PILAR: 6.2.0 - 26.11.2016 PILAR: 5.4.11 - 10.11.2016 PILAR Basic: 5.4.11 - 10.11.2016 microPILAR: 5.4.11 - 10.11.2016 PILAR: 5.4.10 - 14.9.2016 PILAR Basic: 5.4.10 - 14.9.2016 microPILAR: 5.4.10 - 14.9.2016 PILAR: 5.4.9 - 18.7.2015 PILAR Basic: 5.4.9 - 18.7.2015 microPILAR: 5.4.9 - 18.7.2015 PILAR: 5.4.8 - 9.3.2015 PILAR Basic: 5.4.8 - 9.3.2015 microPILAR: 5.4.8 - 9.3.2015 PILAR: 5.4.7 - 12.11.2015 PILAR Basic: 5.4.7 - 12.11.2015 microPILAR: 5.4.7 - 12.11.2015		SimpleRisk v.20170312-001 SimpleRisk v.20170108-001 SimpleRisk v.20170102-001 SimpleRisk v.20161122-001 SimpleRisk v.20161030-001 SimpleRisk v.20161023-001 SimpleRisk v.20160612-001 SimpleRisk v.20160331-001 SimpleRisk v.20160124-001 SimpleRisk v.20151219-001 SimpleRisk v.20151108-001 SimpleRisk v.20150930-001 SimpleRisk v.20150928-001 SimpleRisk v.20150920-001 SimpleRisk v.20150729-001 SimpleRisk v.20150531-001 SimpleRisk v.20150321-001 SimpleRisk v.20150202-001 SimpleRisk v.20141214-001

			PILAR: 5.4.6 - 26.10.2015 PILAR Basic: 5.4.6 - 26.10.2015 microPILAR: 5.4.6 - 26.10.2015 PILAR: 5.4.5 - 13.3.2015 PILAR Basic: 5.4.5 - 13.3.2015 microPILAR: 5.4.5 - 13.3.2015 PILAR: 5.4.4 - 3.12.2014 PILAR Basic: 5.4.4 - 3.12.2014 microPILAR: 5.4.4 - 3.12.2014 RMAT: 5.4.1 - 31.7.2014 PILAR: 5.4.3 - 18.7.2014 PILAR Basic: 5.4.3 - 18.7.2014 microPILAR: 5.4.3 - 18.7.2014 PILAR: 5.4.2 - 30.6.2014 PILAR Basic: 5.4.2 - 30.6.2014 microPILAR: 5.4.2 - 30.6.2014 PILAR: 5.4.1 - 8.4.2014 PILAR Basic: 5.4.1 - 8.4.2014 microPILAR: 5.4.1 - 8.4.2014		SimpleRisk v.20141129-001 SimpleRisk v.20141013-001 SimpleRisk v.20140728-001 SimpleRisk v.20140526-001 SimpleRisk v.20140413-001 SimpleRisk v.20140224-001 SimpleRisk v.20131231-001 SimpleRisk v.20131117-001 SimpleRisk v.20131024-001 SimpleRisk v.20130929-001 SimpleRisk v.20130916-001 SimpleRisk v.20130915-001 SimpleRisk v.20130827-001 SimpleRisk v.20130718-001 SimpleRisk v.20130501-001 SimpleRisk v.20130415-001 SimpleRisk v.20130319-001 SimpleRisk v.20130915-001

			PILAR: 5.4.0 - 12.2.2014 PILAR Basic: 5.4.0 - 12.2.2014 microPILAR: 5.4.0 - 12.2.2014 RMAT: 5.4.0 - 31.1.2014 PILAR: 5.3.2 - 14.1.2014 PILAR Basic: 5.3.2 - 14.1.2014 microPILAR: 5.3.2 - 14.1.2014 RMAT: 5.3.0 - 3.1.2014 PILAR: 5.3.1 - 9.12.2013 PILAR Basic: 5.3.1 - 9.12.2013 microPILAR: 5.3.1 - 9.12.2013 PILAR: 5.3.0 - 12.11.2013 PILAR Basic: 5.3.0 - 12.11.2013 microPILAR: 5.3.0 - 12.11.2013 RMAT: 5.2 - 16.12.2012 PILAR: 5.2.9 - 26.12.2012 PILAR: 5.2.8 - 17.12.2012 PILAR: 5.2.7 - 10.12.2012 PILAR: 5.2.6 - 12.11.2012		

			PILAR: 5.2.5 - 28.9.2012 PILAR: 5.2.4 - 18.9.2012 PILAR: 5.2.3 - 28.8.2012 PILAR: 5.2.2 - 6.8.2012 PILAR: 5.2.1 - 31.7.2012 PILAR: 5.2 - 23.7.2012 PILAR: 5.1.7 - 26.4.2011 PILAR: 5.1.6 - 3.11.2011 PILAR: 4.4.6 - 3.11.2011 PILAR: 5.1.5 - 17.10.2011 PILAR: 5.1.4 - 26.9.2011 RMAT: 5.1 - 12.8.2011 PILAR Basic: 5.1.3 - 13.7.2011 microPILAR : 5.1.3 - 13.7.2011 PILAR : 5.1.2 - 1.6.2011 PILAR Basic: 5.1.2 - 1.6.2011 microPILAR : 5.1.2 - 1.6.2011 PILAR : 5.1.1 - 23.5.2011 PILAR Basic: 5.1.1 - 23.5.2011		

			microPILAR : 5.1.1 - 23.5.2011 PILAR : 5.1 - 28.3.2011 PILAR Basic: 5.1 - 28.3.2011 microPILAR : 5.1 - 28.3.2011 PILAR : 4.4.5 - 1.12.2010 PILAR: 4.4.4 - 16.10.2010 RMAT: 4.4 - 16.10.2010 PILAR: 4.4.3 - 1.7.2010 PILAR: 4.4.2 - 24.2.2010 PILAR & Pilar Basic: 4.4.1 - 8.2.2010 PILAR & Pilar Basic: 4.4 - 1.2.2010 PILAR & Pilar Basic 4.3 - 22.1.2009 RMAT 4.3 - 22.1.2009 PILAR & Pilar Basic 4.2 - 8.7.2008 PILAR & Pilar Basic 4.1.4 - 4.4.2008 PILAR 4.1.3 - 31.3.2008 RMAT 4.1 - 24.3.2008		

				PILAR 4.1.2 - 14.3.2008 PILAR & Pilar Basic 4.1.1 - 25.2.2008 PILAR & Pilar Basic 4.1 - 27.12.2007 PILAR 3.3 - 10.3.2007 PILAR 3.2 - 5.12.2006 PILAR 3.1 - 20.5.2006 PILAR 2.2.10 - 12.12.2005 PILAR 2.2.9 - 30.11.2005 PILAR 2.2.6 - 11.10.2005 PILAR 2.2.5 - 4.10.2005 PILAR 2.2 - 31.10.2005 PILAR 1.2 - 29.11.2004		
Años en el mercado		Función OBA	Atributos relacionados con los años en el mercado del software			
	Número de años del producto en el mercado	Cantidad: Número, Cantidad = Int	Número de años que ha estado el software en el mercado	13	1	4
Tolerancia a fallos		Función OBA	ISO/IEC 9126			

Alertas del sistema		Función OBA	Atributos relacionados con las alertas del sistema			
	Datos incorrectos	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de alerta sobre datos incorrectos	x		x
	Errores del sistema	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad sobre alertas sobre errores del sistema	x	x	x
Recuperabilidad		Función OBA	ISO/IEC 9126			
	Datos del sistema	Función OBA	Atributos relacionados con datos del sistema			
	Restauración de datos luego de una falla	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de restauración de datos luego de una falla		x	
Usabilidad		Función OBA	ISO/IEC 9126			
Aprendizaje		Función OBA	ISO/IEC 9126			
	Facilidad de Idioma	Función OBA	Atributos relacionados con los idiomas del software			
	Español	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que el software soporte el idioma español	x	x	x
	Inglés	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que el software soporte el idioma inglés	x		x
	Francés	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que el software soporte el idioma francés			x

	Italiano	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que el software soporte el idioma italiano	x		x
	Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que el software soporte otros idiomas			x
Facilidad de Nombres		Función OBA	Atributos relacionados con los nombres de las herramientas			
	Nombres nemotécnicos en las herramientas	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de nombres nemotécnicos de las herramientas del software	x	x	x
Comprensión		Función OBA	ISO/IEC 9126			
	Manejo de Iconografía Estándar	Función OBA	Atributos relacionados con el manejo de iconografía de las herramientas del software			
	Lista de Iconos comunes	Iconos: Conjunto (Etiqueta, Nominal), Etiqueta = (guardar, deshacer, ...)	Lista de íconos estandarizados (imprimir, guardar, zoom, etc.)	Nuevo Abrir Guardar Cortar Copiar Pegar Ayuda Importar Exportar	Guardar Copiar Cortar Pegar Hacer Deshacer Buscar	Buscar Guardar Editar Eliminar

Herramientas	Función OBA	Atributos relacionados con las herramientas del software			
Despliegue inmediato sobre información de herramientas	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que la información de la herramienta.	x	x	
Descripción de resultados	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que la herramienta describa el resultado que se va a obtener con su uso	x	x	
Descripción de errores	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que la herramienta describa el error si se llega a presentar	x		x
Operatividad	Función OBA	ISO/IEC 9126			
Facilidad de pasos	Función OBA	Atributos relacionados a la facilidad de pasos para realizar usar herramientas			
Número de pasos para registrar activos	Cantidad: Número, Cantidad = Int	Número de pasos para el registro de un activo de información	6	3	4
Número de pasos para registrar amenazas	Cantidad: Número, Cantidad = Int	Número de pasos para el registro de una amenaza	5	3	4
Número de pasos para registrar contramedidas	Cantidad: Número, Cantidad = Int	Número de pasos para el registro de una contramedida	6	0	5

Número de pasos para calcular el riesgo absoluto	Cantidad: Número, Cantidad = Int	Número de pasos para el cálculo del riesgo absoluto	3	3	3
Número de pasos para calcular riesgo residual	Cantidad: Número, Cantidad = Int	Número de pasos para el cálculo del riesgo residual	3	0	0
Número de pasos para generar informes	Cantidad: Número, Cantidad = Int	Número de pasos para generar informes	3	1	2

Eficiencia	Función OBA	ISO/IEC 9126			
Comportamiento de recursos	Función OBA	ISO/IEC 9126			
Despliegue	Función OBA	Atributos relacionados con el despliegue en el comportamiento de recursos			
Recursos hardware necesarios	Recursos: Conjunto (RAM, Procesador, ...)	Lista de recursos necesarios de hardware (RAM, procesador, etc.)	-Procesador i3. -Disco 500gb. -RAM 4gb. -Tarjeta de red wifi.	Procesador i3 -Disco 500gb. -RAM 4gb.	-Procesador i3. -Disco 500gb. -RAM 4gb. -Tarjeta de red wifi.
Recursos software necesarios	Recursos: Conjunto (OS, Base de datos, ...)	Lista de recursos necesarios de software (OS, Base de datos, etc.)	-JRE-entorno java -Microsoft Office -MySQL	-Microsoft Office	-WPServer -Apache -MySQL -Navegador -Microsoft Office

Ejecución	Función OBA	Atributos relacionados con el tiempo de ejecución en el comportamiento de recursos			
Porcentaje de uso de memoria	Porcentaje: Cantidad, Porcentaje = Float	Porcentaje de RAM que se consume	3,10%	2,20%	3,40%
Porcentaje de uso de disco	Porcentaje: Cantidad, Porcentaje = Float	Porcentaje de disco duro que se consume	0%	0%	0%
Porcentaje de uso de CPU	Porcentaje: Cantidad, Porcentaje = Float	Porcentaje de uso de procesador	0%-1%	0%-1%	0%-1%
Mantenibilidad	Función OBA	ISO/IEC 9126			
Facilidad de análisis	Función OBA	ISO/IEC 9126			
Documentación de Desarrollo	Función OBA	Atributos relacionados con la documentación de desarrollo			
Manual de usuario	Contenido: Nominal, Contenido = (No provee, básico, medio, avanzado)	La categoría en que el manual de usuario está (no provee, básico, medio, avanzado)	avanzado	avanzado	avanzado
Ayuda online	Contenido: Nominal, Contenido = (No provee, básico, medio, avanzado)	La categoría en que la ayuda online está (no provee, básico, medio, avanzado)	avanzado	medio	avanzado
Ventanas de ayuda	Contenido: Nominal, Contenido = (No provee, básico, medio, avanzado)	La categoría en que las ventanas de ayuda están (no provee, básico, medio, avanzado)	avanzado	no provee	no provee

Portabilidad	Función OBA	ISO/IEC 9126			
Capacidad de instalación	Función OBA	ISO/IEC 9126			
Facilidad de instalación	Función OBA	Atributos relacionados con la facilidad de instalación			
Tiempo promedio de instalación	Tiempo: Numero, Tiempo = Float	Tiempo promedio que se tarda en la instalación	30s	0m	20m
Número de pasos de instalación	Cantidad: Número, Cantidad = Int	Número de pasos necesarios para realizar la instalación	5	0	7
Recursos utilizados en instalación	Función OBA	Atributos relacionados con los recursos para la capacidad de instalación			
Porcentaje de uso de memoria	Porcentaje: Cantidad, Porcentaje = Float	Porcentaje de uso de RAM en la instalación	0,90%	0%	0,60%
Porcentaje de uso de disco	Porcentaje: Cantidad, Porcentaje = Float	Porcentaje de uso de disco en la instalación	0%	0%	0%
Porcentaje de uso de CPU	Porcentaje: Cantidad, Porcentaje = Float	Porcentaje de uso de procesador en la instalación	0%	0%	0%
Transportabilidad	Función OBA	ISO/IEC 9126			
Plataformas de ejecución	Función OBA	Atributos relacionados a las plataformas de ejecución			
Sistemas Operativos	Función OBA	Atributos relacionados con los sistemas operativos con los cuales se puede trabajar			

Windows	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que el software corra en sistema operativo Windows	x	x	x
Mac	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que el software corra en sistema operativo Mac	x	x	x
Linux	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que el software corra en sistema operativo Linux	x	x	x
Otros	Soportado: Nominal; Soportado=(Verdadero, Falso)	Posibilidad de que el software corra en otro sistema operativo		x	x

3.6. Análisis de resultados

A continuación, se presentará un cuadro de resumen con los resultados obtenidos de la aplicación de la evaluación de software realizado en las tres herramientas de gestión de riesgos.

				EAR/PILAR	Análisis de riesgos INCIBE	SimpleRisk
Funcionalidad	**Adecuación**	Gestión de activos de información	Registro de activos de información	El software cumple con la mayoría de categorías y subcategorías de activos que se evalúan en el plan. También da la posibilidad de añadir más categorías y subcategorías que las que el software ofrece por defecto.	La herramienta cumple con pocos de los atributos de los atributos evaluados, debido a que no proporciona categorías ni subcategorías específicas para registrar los activos, sin embargo, se puede crear dichas categorías y subcategorías según sea los requerimientos del usuario.	El software cumple con pocos de los atributos evaluados, debido a que no proporciona categorías ni subcategorías específicas para registrar los activos, sin embargo, se puede crear dichas categorías y subcategorías según sea los requerimientos del usuario.
			Valoración de activos de información	El software cumple con todos los atributos de valoración evaluados, debido a que cumple valoración de Disponibilidad, Integridad y Confidencialidad.	La herramienta no cumple con la valoración de activos de ninguna manera.	El software cumple con uno de los atributos evaluados, debido a que no evalúa a los activos en criterios de Disponibilidad, Integridad o Confidencialidad, en cambio valora el activo en dinero.
		Gestión de amenazas	Registro de amenazas	El software cumple con todos los atributos evaluados debido a que cuenta con todas las	La herramienta cumple con todos los atributos evaluados debido a que cuenta con todas las	El software cumple con todos los atributos evaluados debido a que cuenta con todas las

				categorías de amenazas evaluadas.	categorías de amenazas evaluadas.	categorías de amenazas evaluadas.
			Valoración de amenazas	El software cumple con todos los atributos de valoración evaluados, debido a que cumple valoración de Disponibilidad, Integridad y Confidencialidad.	El software cumple con uno de los atributos evaluados, debido a que no evalúa a los activos en criterios de Disponibilidad, Integridad o Confidencialidad, en cambio, los valora por el impacto y probabilidad.	El software cumple con todos de los atributos de valoración evaluados, debido a que cumple valoración de Disponibilidad, Integridad y Confidencialidad.
		Gestión de contramedidas	Registro de contramedidas	El software cumple con todos los atributos evaluados debido a que cuenta con todas las categorías contramedidas evaluadas.	La herramienta non cuenta con el registro de contramedidas.	El software cumple con uno de los atributos evaluados, debido a que no cumple ninguna categoría de contramedidas evaluadas, pero presenta planes de mitigación asociado a cada amenaza registrada.
			Valoración de contramedidas	El software no cuenta con valoración de Disponibilidad, Integridad o Confidencialidad para las contramedidas, sin embargo, tiene otro tipo de valoración basada en que la contramedida puede ser: inexistente, inicial, reproducible, proceso definido, gestionado y medible,	La herramienta no cuenta con valoración de contramedidas	La valorización del plan de mitigación, se lo realiza en términos monetarios, es decir, cuánto costará implementar dicho plan para contrarrestar el riesgo identificado.

				optimizado o no aplicable. Valorizando el estado actual de la contramedida y el estado al cual se aspira llegar.		
		Análisis de riesgos	Evaluación de probabilidad	El software cuenta con el registro probabilidad que el riesgo pueda ocurrir.	La herramienta cuenta con el registro de la probabilidad que el riesgo pueda ocurrir.	El software cuenta con el registro probabilidad que el riesgo pueda ocurrir.
			Evaluación de consecuencia	El software cuenta con el registro de la consecuencia que ocasionaría si el riesgo se legara a materializar.	La herramienta cuenta con el registro de la consecuencia que ocasionaría si el riesgo se legara a materializar.	El software cuenta con el registro de la consecuencia que ocasionaría si el riesgo se legara a materializar.
			Cálculo de riesgo absoluto	El software hace el cálculo del riesgo absoluto, probabilidad x impacto	La herramienta hace el cálculo del riesgo absoluto, probabilidad x impacto	El software hace el cálculo del riesgo absoluto, probabilidad x impacto
			Cálculo de riesgo residual	El software hace el cálculo de riesgo residual, a partir de las contramedidas registradas y valorizadas.	La herramienta no cuenta con cálculo de riesgo residual, debido a que no cuenta con el registro de las contramedidas.	El software no cuenta con cálculo de riesgo residual, debido a que solo se registra un plan de mitigación valorizado monetariamente, mas no el impacto que tendrá el plan dentro del riesgo.
			Valorar de riesgo	El software valora el riesgo que ha sido calculado anteriormente, es decir, si la amenaza es un riesgo extremo, alto, medio, etc. Dependiendo	La herramienta valora el riesgo que ha sido calculado anteriormente, es decir, si la amenaza es un riesgo extremo, alto, medio, etc. Dependiendo	El software valora el riesgo que ha sido calculado anteriormente, es decir, si la amenaza es un riesgo extremo, alto, medio, etc.

				de la metodología utilizada.	de la metodología utilizada.	Dependiendo de la metodología utilizada.
		Generación de informes	Análisis de riesgos	El software, genera informe de análisis de riesgos, presentado cada uno de los riesgos registrados, y a qué activos afecta.	La herramienta presenta este informe, a partir del cálculo del riesgo absoluto.	El software, genera informe de análisis de riesgos, presentado cada uno de los riesgos registrados, y a qué activos afecta.
			Informe de amenazas	El software informa al usuario acerca de todas las amenazas que están latentes en su empresa.	La herramienta presenta este informe dentro, a partir del cálculo del riesgo absoluto.	El software informa al usuario acerca de todas las amenazas que están latentes en su empresa.
			Otros	El software tiene otro tipo de informes como: análisis de impacto en el negocio, resumen de continuidad del negocio, evaluación de las salvaguardias, etc.	La herramienta no contempla otro tipo de informes	El software tiene otro tipo de informes como: tendencia de riesgo, promedio de riesgo en el tiempo, informe de alto riesgo, etc.
	Exactitud	Herramientas de cálculo de riesgos	Cálculo de riesgo absoluto	El software calcula con 0% de error el valor del riesgo absoluto, las pruebas se realizaron multiplicando el impacto por el riesgo.	La herramienta calcula con 0% de error el valor del riesgo absoluto, las pruebas se realizaron multiplicando el impacto por el riesgo.	El software calcula con 0% de error el valor del riesgo absoluto, las pruebas se realizaron multiplicando el impacto por el riesgo.

			Cálculo de riesgo residual	El software calcula con 0% de error el valor del riesgo residual, las pruebas se realizaron multiplicando el impacto por el riesgo después de la aplicación de contramedidas.	La herramienta no cuenta con cálculo de riesgo residual, debido a que no cuenta con el registro de las contramedidas.	El software no cuenta con cálculo de riesgo residual, debido a que solo se registra un plan de mitigación valorizado monetariamente, mas no el impacto que tendrá el plan dentro del riesgo.
	Interoperabilidad	Interoperabilidad de archivos	Importar archivos	El software cumple con la importación de todos los archivos que se evalúan.	La herramienta al ser desarrollada en Microsoft Excel puede trabajar con archivos tipo csv, xml, xlsx, etc.	El software permite importar archivos de tipo csv.
			Exportabilidad de archivos	El software cumple 100% con la exportación de todos los tipos de archivos evaluados.	La herramienta genera archivos de tipo csv, y otros como pdf, xlsx, xml, etc.	El software permite exportar archivos de tipo csv.
	Seguridad	Usuarios		El software en su versión de prueba no presenta autenticación de usuario.	La herramienta no cuenta con autenticación de usuario.	El software cuenta con autenticación de usuario.
		Permisos de usuarios		Todas las personas que entran al sistema pueden modificarlo a voluntad.	No cuenta con permisos específicos de usuario, sin embargo, se puede proteger los archivos con contraseñas para que solo las personas autorizadas modifiquen el archivo.	En el software a los usuarios se les asignan diferentes permisos, dependiendo del tipo de usuario.
		Registro de actividad		No cuenta con un registro de actividad.	No cuenta con un registro de actividad.	Cuenta con un registro de actividad, en el cual se puede saber qué usuario modificó los datos del software.

		Acceso al código fuente		No se permite acceso al código fuente	No se permite modificar las sentencias de la herramienta.	Permite el acceso al código fuente.
		Ubicación de los directorios		Se conoce la ubicación de los directorios	Es un archivo de Microsoft Excel, fácilmente detectable en un ataque.	Se conoce la ubicación de los directorios
Fiabilidad	**Madurez**	Versiones	Lista de versiones del producto	El software desde su lanzamiento en 2004 hasta la actualidad (2017) tiene un total de 112 versiones, entre las cuales van correcciones de errores, lanzamientos de nuevas funcionalidades, mejoras, etc.	La herramienta cuenta con una sola versión que proporciona INCIBE.	El software registra desde su lanzamiento en 2013 hasta la actualidad (2017) un total de 41 versiones.
		Años en el mercado	Número de años en el mercado	El software se encuentra en el mercado alrededor de 13 años, y se ha posicionado como uno de los softwares más estables en gestión de riesgos.	La herramienta cuenta con un año desde su lanzamiento en el análisis de riesgos de INCIBE.	El software está en el mercado alrededor de 4 años, y poco a poco se ha ido posicionando por lo que ofrece a los clientes y la facilidad de uso.
	Tolerancia a fallos	Alertas del sistema	Datos incorrectos	El software lanza advertencias sobre datos incorrectos, es decir, valida la entrada de datos.	La herramienta no lanza advertencias sobre datos incorrectos. Sin embargo, se podría implementar validaciones en la herramienta.	El software lanza advertencias sobre datos incorrectos, aunque, la mayoría de validación en la entrada de datos se los hace por medio de listas, en las cuales el usuario no debe digitar datos, sino escoger opciones de una lista definida, evitando la

						digitación de datos incorrectos.
			Errores del sistema	Informa al usuario acerca de errores producidos en el sistema, mediante un Log Window, o ventana de seguimiento, en la cual se informa acerca de errores, advertencias o informaciones que se susciten, en el funcionamiento del software.	Microsoft Excel lanza una advertencia acerca de un error en alguna celda si algún dato es incorrecto y no sirve para el funcionamiento de la herramienta.	El software informa al usuario acerca del error que se haya ocurrido mediante un mensaje dentro del software.
	Recuperabilidad	Datos del sistema	Restauración de datos luego de una falla	Los datos que no hayan sido guardados antes que ocurra una falla con el software se perderán. Esta prueba se realizó con el cierre intempestivo del software y con apagándose la computadora intempestivamente.	Microsoft Excel puede recuperar los datos que no hayan sido guardados. Esta prueba se realizó con el cierre intempestivo del software y con apagándose la computadora intempestivamente.	Los datos que no hayan sido guardados antes que ocurra una falla con el software se perderán. Esta prueba se realizó con el cierre intempestivo del software y con apagándose la computadora intempestivamente.
Usabilidad	**Aprendizaje**	Facilidad de idioma	Español	El software está disponible en una versión en español.	La herramienta está disponible en idioma español.	El software está disponible en una versión en español.
			Inglés	El software está disponible en una versión en inglés.	La herramienta no está disponible en inglés.	El software está disponible en una versión en inglés.
			Francés	El software no tiene la posibilidad del idioma francés.	La herramienta no está disponible en francés	El software está disponible en una versión en francés.

			Italiano	El software está disponible en una versión en italiano.	La herramienta no está disponible en inglés.	El software está disponible en una versión en italiano.
			Otros	El software no soporta otros idiomas.	La herramienta no está disponible en otros idiomas.	El software puede trabajar con otros idiomas como: catalán, portugués, ruso, alemán, turco, etc.
		Facilidad de nombres	Nombres nemotécnicos en las herramientas	El software presenta nombres nemotécnicos en las herramientas, ya que son fáciles de aprender y muy intuitivos acerca de su funcionamiento.	La herramienta presenta nombres nemotécnicos en sus funciones, son fáciles de aprender y muy intuitivos.	El software presenta nombres nemotécnicos en las herramientas, ya que son fáciles de aprender y muy intuitivos acerca de su funcionamiento.
	Comprensión	Manejo de iconografía estándar	Lista de íconos comunes	El software presenta una lista de íconos estándar, conocidos y utilizados por los usuarios, por lo que son fácilmente reconocibles.	La herramienta presenta una lista de íconos estándar, conocidos y utilizados por los usuarios, por lo que son fácilmente reconocibles.	El software presenta una lista de íconos estándar, conocidos y utilizados por los usuarios, por lo que son fácilmente reconocibles.
		Herramientas	Despliegue inmediato sobre información de herramientas	El software ofrece información sobre las herramientas que se usan, redirigiendo a una página de ayuda en línea en donde se puede consultar a cerca de cómo funciona la herramienta.	La herramienta ofrece información del funcionamiento de cada una de las partes que la conforman.	El software no ofrece información acerca de las herramientas que utiliza.
			Descripción de resultados	El software describe qué resultados se van a obtener por la aplicación de cualquier herramienta,	La herramienta describe los resultados que se van a obtener en cada una de las funcionalidades de la misma.	El software no dispone de descripción de resultados.

				lo hace a través de una página de ayuda en línea.		
			Descripción de errores	El software describe los errores que se puedan suscitar a través de su ventana de seguimiento.	La herramienta no describe los errores suscitados.	El software describe los errores que se puedan suscitar, a través de mensajes.
	Operatividad	Facilidad de pasos	Número de pasos para registrar activos	1. Elegir proyecto. 2. Elegir Análisis de riesgo/Activos/Identificación. 3. Escoger grupo de activos o crear grupo. 4. Elegir la opción nuevo activo. 5. Llenar información de activo. 6. Guardar.	1. Elegir la opción de registro de activos. 2. Elegir la aplicación o no del activo. 3. Guardar.	1. Elegir gestión de activos. 2. Elegir la opción añadir o eliminar activos. 3. Llenar la información del activo. 4. Guardar
			Número de pasos para registrar amenazas	1. Elegir proyecto 2. Elegir Análisis de riesgo/Amenazas/Identificación. 3. Escoger categoría de amenazas. 4. Elegir activo y escoger a qué amenaza relacionar. 5. Guardar.	1. Elegir la opción de registro de cruce activo-amenazas 2. Elegir la aplicación o no la amenaza sobre el activo. 3. Guardar.	1. Elegir gestión de riesgos. 2. Elegir riesgo de presentar. 3. Llenar la información del riesgo. 4. Guardar.
			Número de pasos para registrar contramedidas	1. Elegir proyecto 2. Elegir Análisis de riesgo/Salvaguardas/Identificación. 3. Escoger categoría de salvaguarda. 4. Llenar datos de	La herramienta no cuenta con registro de contramedidas.	1. Elegir gestión de riesgos. 2. Elegir plan de mitigación. 3. Elegir amenaza que se requiera mitigar. 4. Llenar información de

				contramedida. 5. Relacionar con amenaza. 6. Guardar.		plan de mitigación. 5. Guardar.
			Número de pasos para calcular el riesgo absoluto	1. Elegir proyecto 2. Elegir Análisis de riesgo/Impacto y riesgos residuales/ Valores acumulados Riesgo. 3. Escoger riesgo.	1. Elegir la opción de registro análisis de riesgos. 2. Elegir la opción mostrar activos. 3. Valorar la probabilidad e impacto del riesgo.	1. Elegir evaluaciones. 2. Elegir evaluaciones disponibles. 3. Elegir riesgo.
			Número de pasos para calcular riesgo residual	1. Elegir proyecto 2. Elegir Análisis de riesgo/Impacto y riesgos residuales/ Valores repercutidos/ Riesgo. 3. Escoger riesgo.	La herramienta no cuenta con cálculo de riesgos residuales.	El software no cuenta con cálculo de riesgos residuales.
			Número de pasos para generar informes	1. Elegir proyecto 2. Elegir Informes/ R.r textuales 3. Escoger informe.	1. Elegir la opción de registro análisis de riesgos.	1. Elegir reportes. 2. Elegir informe.
Eficiencia	**Comportamiento de recursos**	Despliegue	Recursos necesarios de hardware	El software necesita recursos hardware considerado básicos en la actualidad: Procesador Core i3. Disco duro de 500 GB. Memoria RAM 4GB. Tarjeta de Red.	La herramienta necesita recursos hardware considerado básicos en la actualidad: Procesador Core i3. Disco duro de 500 GB. Memoria RAM 4GB.	El software necesita recursos hardware considerado básicos en la actualidad: Procesador Core i3. Disco duro de 500 GB. Memoria RAM 4GB. Tarjeta de Red.

			Recursos necesarios de software	Se requieren las siguientes herramientas de software: JRE un entorno de java. Microsoft Office. En caso de contar con la versión completa de software se puede escoger tener una base de datos MySQL.	Se requiere Microsoft Office para que la herramienta funcione.	Se requieren las siguientes herramientas de software: -WAMPServer para montar un Host Virtual. -Apache. -Base de datos MySQL Microsoft Office.
		Ejecución	Porcentaje de uso de memoria	El software presenta un promedio de porcentaje de uso de memoria RAM de 3,10% después de realizar pruebas de funcionamiento.	El software presenta un promedio de porcentaje de uso de memoria RAM de 2,20% después de realizar pruebas de funcionamiento.	El software presenta un promedio de porcentaje de uso de memoria RAM de 3,40% después de realizar pruebas de funcionamiento.
			Porcentaje de uso de disco	El software presenta un promedio de porcentaje de uso de disco duro 0%, después de realizar las pruebas de funcionamiento.	La herramienta presenta un promedio de porcentaje de uso de disco duro 0%, después de realizar las pruebas de funcionamiento.	El software presenta un promedio de porcentaje de uso de disco duro 0%, después de realizar las pruebas de funcionamiento.
			Porcentaje de uso de CPU	El software presenta un promedio de porcentaje de uso de procesador una cantidad que oscila 0% a 1%, después de realizar las pruebas de funcionamiento.	La herramienta presenta un promedio de porcentaje de uso de procesador una cantidad que oscila 0% a 1%, después de realizar las pruebas de funcionamiento.	El software presenta un promedio de porcentaje de uso de procesador una cantidad que oscila 0% a 1%, después de realizar las pruebas de funcionamiento.
Mantenibilidad	**Facilidad de análisis**	Documentación de desarrollo	Manual de usuario	El software provee un avanzado manual de usuario dentro de la documentación en su página web.	La herramienta provee un avanzado manual de usuario, con las explicaciones de funcionamiento explicado	El software provee un avanzado manual de usuario dentro de la documentación en su página web.

					dentro de la propia herramienta.	
			Ayuda online	El software provee una avanzada ayuda online que se encuentra dentro de su página web, EAR/PILAR ofrece soporte técnico.	La herramienta proporciona un medio nivel de ayuda online, ya que en la página de INCIBE se explica cómo gestionar los riesgos de información.	El software provee una avanzada ayuda online que se encuentra dentro de su página web, SimpleRisk ofrece soporte técnico.
			Ventanas de ayuda	El software provee ventanas de ayuda en la cual se puede consultar y solucionar dudas acerca del funcionamiento de la herramienta.	La herramienta no provee ventanas de ayuda.	El software no provee ventanas de ayuda.
Portabilidad	**Capacidad de instalación**	Facilidad de instalación	Tiempo promedio de instalación	El tiempo promedio de instalación del software es 30 segundos, desde el momento que se ejecuta el instalador hasta que finalice todas las configuraciones.	El tiempo promedio de instalación de la herramienta es 0 segundos, debido a que es un archivo de tipo Excel y se lo ejecuta directamente.	El tiempo promedio de instalación del software y todos sus recursos necesarios son 20 minutos, realizando todas las configuraciones.
			Número de pasos de instalación	1. Descargar instalador de PILAR 2. Solicitar licencia de prueba. 3. Ejecutar instalador de PILAR. 4. Realizar configuraciones de PILAR. 5. Activar licencia de	Solo se necesita abrir el archivo descargado.	1. Descargar e instalar WAMPSERVER 2. Descargar archivos de SimpleRisk. 3. Crear un VirtualHost en WAMPSERVER. 4. Configurar MySQL desde WAMPSERVER. 5. Ejecutar el instalador de SimpleRisk desde el navegador.

				evaluación.		6. Configurar el archivo My.ini de MySQL 7. Guardar configuraciones.
		Recursos utilizados en instalación	Porcentaje de uso de memoria	El porcentaje promedio de uso de memoria RAM en la instalación del software es 0,90%,	No se instala la herramienta.	El porcentaje promedio de uso de memoria RAM en la instalación del software es 0,60%,
			Porcentaje de uso de disco	El porcentaje promedio de uso de disco duro en la instalación del software es 0%,	No se instala la herramienta.	El porcentaje promedio de uso de disco duro en la instalación del software es 0%,
			Porcentaje de uso de CPU	El porcentaje promedio de uso del procesador en la instalación del software es 0%,	No se instala la herramienta.	El porcentaje promedio de uso del procesador en la instalación del software es 0%-2% debido al proceso de instalación de todos los recursos de software necesarios para que SimpleRisk esté en funcionamiento,
	Transportabilidad	Plataformas de ejecución	Sistemas Operativos	El software puede funcionar en Windows, Linux y Mac	La herramienta puede funcionar en cualquier sistema operativo siempre y cuando esté instalado Microsoft Office.	El software funciona en cualquier plataforma de manera local, siempre y cuando se pueda instalar un Host Virtual, y se maneje base de datos MySQL, también puede funcionar en cualquier plataforma si se contrata el servicio Hosted de SimpleRisk.

3.7. Conclusiones de sección de análisis de software

El estándar de calidad ISO/IEC 9126 facilita las directrices para desarrollar una guía de evaluación de software, la cual puede ser elaborada de acuerdo a las necesidades del dominio de software que se requiera analizar.

El software PILAR es una herramienta consolidada que hasta el día de hoy sigue vigente y en constante evolución; presenta una funcionalidad muy intuitiva, fácil de reconocer y aplicar, ideal para empresas MPYMES, ya que su costo de adquisición es relativamente bajo comparándolo con otros paquetes comerciales de gestión de riesgos.

SimpleRisk es una muy buena herramienta de código abierto para gestión de riesgos, la cual ha recibido muy buenas críticas desde su lanzamiento en la conferencia de seguridad BSides Austin del año 2013. La herramienta es fácil de usar y de entender, además cuenta con adaptabilidad para varios idiomas, y una interfaz gráfica simple, lo que la hace fuerte en aspectos de interacción con los usuarios, el costo de obtener la herramienta es un poco elevado, sin embargo, una buena gestión de riesgos para una empresa puede significar ahorro de dinero a lo largo del tiempo.

La guía de análisis de riesgos proporcionada por el Instituto de Ciberseguridad (INCIBE), es una muy buena herramienta para la introducirse en el ámbito de la seguridad, y más específicamente en la gestión de riesgos, ya que en ella se puede aprender a identificar activos e identificar y valorar riesgos, con el fin de crear una conciencia de seguridad en las empresas.

La seguridad de SimpleRisk en su software es muy importante, ya que cuida que los datos solo sean modificados por las personas autorizadas, y es un factor que se debería implementar en todas las herramientas de gestión de riesgos.

La guía de evaluación fue realizada en base al funcionamiento de la metodología Ecu@Risk, la herramienta que más atributos cumple dentro de la evaluación aplicada, fue EAR/PILAR, por lo tanto, su estructura y funcionamiento puede ser planteada como la base para el desarrollo del software para la metodología Ecu@Risk.

Se debe mejorar la interfaz del software para que sea más intuitivo y fácil para el usuario poder manejar y aprender la herramienta, SimpleRisk presenta esta característica debido a que posee una interfaz gráfica muy sencilla y completa a la vez, por lo que se tomará en cuenta dicho detalle para la construcción del software de la metodología Ecu@Risk.

En la actualidad la seguridad de la información juega un papel muy importante dentro de las empresas, no contar con la misma, las informaciones de las organizaciones estuvieran propensas a pérdidas, robos, falsificaciones, clonaciones, etc. Un sinfín de riesgos que podrían desatar consecuencias muy graves para las organizaciones y sus respectivos negocios. Se debe concientizar a acerca de la protección de la información, ya que es un recurso vital para las empresas; una forma es contar con la ayuda de herramientas que permitan la prevención, el control, la reducción y la mitigación de los riesgos, dichas herramientas son efectivas pero su uso no es muy común en el mercado ecuatoriano debido a falta de conciencia de seguridad o que muchas de las veces se coloca al factor económico como un impedimento para la adquisición de dichas herramientas, sin embargo, la protección de la información no significa un gasto, más bien es una inversión que traerá múltiples beneficios y seguridad a la empresa.

Levantamiento de requerimientos

3.8. Introducción

En el presente documento se detallan las especificaciones y requerimientos necesarios del software para la metodología Ecu@Risk; todas las descripciones detalladas del software realizadas en este apartado, servirán como guía para las etapas posteriores de diseño y construcción del mismo.

Se describe el ámbito del software, así también cómo será su funcionalidad, y los usuarios que lo manipulará, es decir, se detalla todo aspecto del software que se plantea desarrollar. Para el levantamiento de requisitos se referencia el estándar IEEE 830, además para el análisis y presentación de las especificaciones se realiza empleando el Lenguaje de Modelado Unificado (UML).

3.9. Propósito

El propósito de este documento es definir las especificaciones funcionales y no funcionales para el desarrollo de un sistema web que permita gestionar riesgos de los activos de información de una empresa basado en la aplicación de la metodología Ecu@Risk de gestión de riesgos de información. Este sistema será utilizado por la empresa y su personal.

3.10. Ámbito del Sistema

El nombre del sistema será Ecu@Risk.

Se contempla que el sistema maneje:

- Inicio de sesión/Cierre de sesión de usuarios.
- Verificación de usuario con clave token.
- Gestión de usuarios: creación y modificación de usuarios del sistema.
- Gestión de activos de información: registrar, modificar y valorar activos de información de la empresa.
- Gestión de amenazas: registrar, modificar y valorar amenazas que puedan atentar en contra de los activos de información.
- Gestión de contramedidas: registrar, modificar y valorar contramedidas que mitiguen a las amenazas que pueden afectar a los activos de información.
- Registro de incidentes: registrar percances que se presenten en la empresa.
- Cálculo de riesgos: riesgo absoluto y riesgo residual.
- Presentación de cuadro de mando integrado (CMI): reportes de riesgos, activos y contramedidas, riesgo absoluto y riesgo residual.
- Gestión de procesos de negocio: creación, modificación y eliminación de procesos y subprocesos de negocio. Asociación de activos de información a procesos.
- Gestión de indicadores clave de desempeño (KPI): creación y modificación de indicadores clave de desempeño, de acuerdo a categorías.

El objetivo que tiene el sistema es proporcionar a las empresas MPYMES una herramienta para que puedan gestionar activos de información, amenazas, riesgos, contramedidas y ofrecer indicadores para la toma de decisiones a nivel de gobierno de seguridad de información.

3.11. Definiciones, Acrónimos y Abreviaturas

Tabla 51:
Definiciones, acrónimos y abreviaturas.

Nombre	***Descripción***
Usuario	Persona que usará el sistema para gestionar procesos
ERS	Especificación de Requisitos Software
RF	Requerimiento Funcional
RNF	Requerimiento No Funcional
CMI	Control de mando integrado
KPI	Indicadores clave de desempeño
ADM	Administrador del sistema
CSD	Coordinador de seguridad designado
CRTI	Comité de riesgo de tecnología de información

Fuente: (IEEE, 2008)

3.12. Referencias

Tabla 52:
Referencias de documentación.

Título del Documento	*Referencia*
Standard IEEE 830 - 1998	IEEE
Ecu@Risk una metodología para la gestión de riesgo.	Ing. Esteban Crespo Martínez.

Fuente: (IEEE, 2008)

3.13. Visión general del documento

El documento se desarrolla en tres secciones. En la primera se da una breve introducción del documento, brindando una visión general sobre las especificaciones del sistema.

La segunda sección del documento se da una descripción generalizada sobre el sistema, mediante el uso de diagramas se especifica las diversas funciones que el poseerá, algunas restricciones, supuestos y factores ligados directamente con el desarrollo.

La última sección de documento consiste en la definición detallada de todos los requerimientos que el sistema deberá cumplir.

3.14. Descripción General

3.14.1. Perspectiva del Producto

El sistema Ecu@Risk será un producto diseñado para trabajar en entornos Web, lo que permitirá su utilización de forma rápida, eficiente y sin restricciones de sistemas operativos o lenguajes de programación. Será un sistema independiente.

3.14.2. Funciones del producto

El sistema tendrá un inicio de sesión en el cual conste de nombre de usuario, contraseña y un token de autenticación.

Se contempla que el sistema registre y actualice activos de información de una empresa, en diferentes categorías: edificaciones, hardware, software, información electrónica, información en papel, medios de almacenamiento extraíble, infraestructura de comunicaciones y recursos humanos. Estos activos se valorizarán, es decir, se pondrá un valor numérico en dimensiones de Disponibilidad, Integridad y Confidencialidad, este valor depende del grado en el que la

empresa resulte afectada si alguna amenaza llegara a materializar el riesgo sobre un activo de información.

Las amenazas que pueden afectar a los activos de información se las registra y actualiza bajo las siguientes categorías: naturales, provocados (deliberados), provocados (por error), informáticos y comunicacionales. Estas amenazas se valorizarán, es decir, se pondrá un valor numérico en número de veces que ha sucedido dicha amenaza (frecuencia) o un valor porcentual de probabilidad que se pueda materializar este riesgo, también se indica si afecta a dimensiones de Disponibilidad, Integridad y Confidencialidad.

El sistema registrará y actualizará salvaguardas o contramedidas que aporten al control de las amenazas encontradas y registradas. Estas contramedidas se valorizarán según la frecuencia con que se presente el riesgo después de haber implementado una contramedida o salvaguarda. La gestión de contramedidas tendrá que también registrar el presupuesto y la inversión para realizar la implementación la contramedida registrada.

El sistema registrará incidentes que se pueden presentarse en la empresa.

Gestión de procesos de negocio: creación, modificación y consulta de procesos de negocio. Posibilidad de asociar los activos de información registrados a procesos de negocio de la organización. Registro de incidentes suscitados dentro del proceso de negocio y que afecten a la organización.

El sistema contendrá un CMI (cuadro de mando integral) que visualice los procesos de negocio, los activos de información involucrados, las amenazas que presentan cada activo, las contramedidas que están actuando para mitigar esa amenaza, y finalmente el riesgo que tiene cada activo representado en forma de semáforo.

El sistema tendrá la generación de reportes de desempeño en base a los KPI (indicadores clave de desempeño) definidos, es decir, se podrá crear un reporte con cualquier indicador designado que se requiera sea este de incidentes, inversiones o procesos de negocio.

Adicionalmente el sistema contempla la gestión de usuarios, en el cual se crea y modifica usuarios para que puedan acceder y manipular la información del sistema. Así también un sistema de seguimiento de actividades de cada uno de los usuarios del sistema de gestión de riesgos.

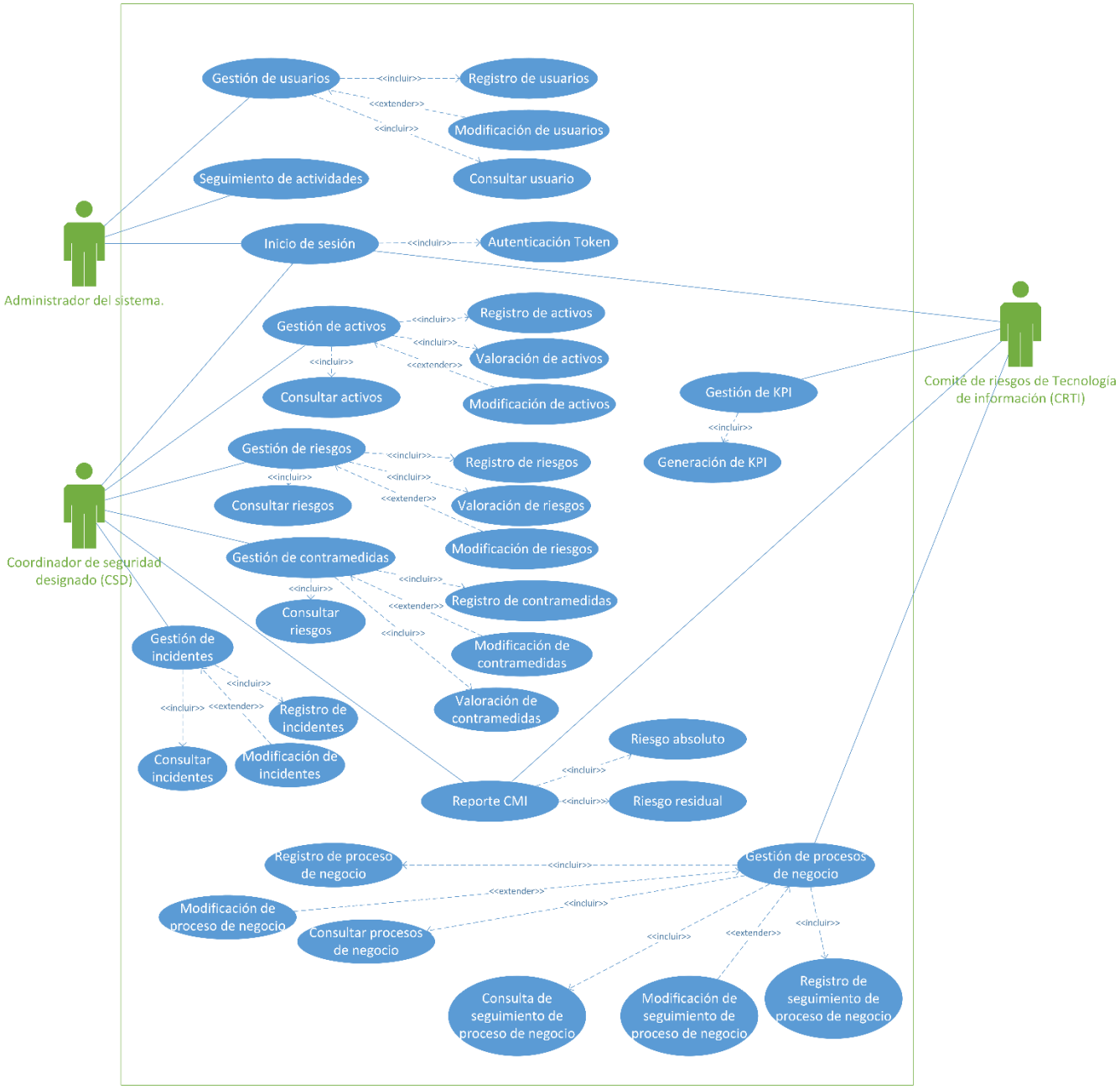

Ilustración 20: Funcionamiento del sistema.
Fuente: Elaboración propia

Características de los usuarios

Tipo de usuario	Administrador del sistema
Formación	Conocimiento de administración de sistemas.
Actividades	Gestión de usuarios. Revisión de actividades de los usuarios.

Tipo de usuario	Coordinador de seguridad designado
Formación	Especialista en gestión de seguridad de la información
Actividades	Registrar activos de información. Modificar activos de información. Valorar activos de información. Registrar amenazas. Modificar amenazas. Valorar amenazas. Registrar planes de tratamiento (contramedidas). Valorar contramedida. Solicitar reporte CMI. Registrar incidentes.

Tipo de usuario	Comité designado de riesgos de tecnología de información
Formación	Conocimiento de procesos de negocio, área a la que pertenecen, unidades estratégicas de negocio.
Actividades	Crear procesos de procesos de negocio. Asociar activos a procesos de negocio. Modificar procesos de negocio. Solicitar reporte CMI. Generar reporte KPI.

3.14.4. Restricciones

- Interfaz sencilla, intuitiva para ser usada en un navegador web.
- Dominio (X) de la empresa.
- El sistema se diseñará con una arquitectura Cliente/Servidor
- El sistema debe tener un diseño e implementación sencillo.
- El sistema debe ser capaz de almacenar una gran cantidad de datos.
- El servidor debe ser capaz de atender grandes consultas de datos.
- Para su construcción se utiliza: NetBeans IDE 8.1 como entorno de desarrollo, JavaSererFaces como framework, GlassFish Server 4.1 como servidor de aplicaciones y MySQL Workbench 6.3 CE como gestor de base de datos.

3.14.5. Suposiciones y dependencias

- Estabilidad en los requerimientos planteados en este documento.
- Equipos en los cuales se ejecuta el sistema, deben cumplir con los requisitos planteados anteriormente para garantizar su ejecución de manera óptima.

3.15. Requisitos Específicos

3.15.1. Interfaces de Usuario

La interfaz de usuario tendrá una estructura fácilmente intuitiva y manejable, conformado por un conjunto de ventanas, listas, botones y cuadros de texto. Esta interfaz será desarrollada para ser visualizada desde un navegador de internet.

3.15.2. Interfaces de hardware

- Servidor:
    - Procesadores: 2x 2.53GHz Intel Xeon Quad-Core E5540.
    - Memoria RAM: 24GB RAM
    - Discos duros:2x 73GB 10K SAS Hard Drives.
- Equipos de cómputo con:
    - Adaptadores de red.
    - Procesador i3.
    - Memoria RAM mínima 1GB.
    - Mouse.
    - Teclado.

3.15.3. Interfaces de software

- Explorador web: mínimo Mozilla 55.0 o mínimo Chrome 60.0.3112.78.

3.15.4. Interfaces de comunicación

Las comunicaciones entre servidores, aplicaciones y clientes se realizarán mediante protocolos estándares de internet como HTTP, SSL, TCP/IP, FTP entre otros.

3.16. Requisitos funcionales

Identificación de caso de uso	CDU01
Nombre	Inicio de sesión.
Actores	Coordinador de seguridad designado, Comité de riesgos de tecnología de información, Administrador del sistema.
Descripción del caso de uso	1.El sistema solicitará ingreso de usuario y contraseña.
Condiciones previas	
Resultado de la terminación	1.Redirección a autenticación por clave token.
Excepciones	1.Usuario o contraseña incorrecta. 1.1Volver a pedir datos

Asociaciones de casos de uso	CDU02
Resumen de entradas	1.Usuario. 2.Contraseña
Resumen de salidas	1.Ingreso exitoso de usuario y contraseña. 2.Autenticación token.

Identificación de caso de uso	CDU02
Nombre	Autenticación Token.
Actores	Coordinador de seguridad designado, Comité de riesgos de tecnología de información.
Descripción del caso de uso	1.El sistema solicitará una autenticación con una clave token. 2.Usuario debe solicitar clave a través de la aplicación Google Autheticator. 3.Ingresar la clave token.
Condiciones previas	1.Usuario y contraseña correctos. 2.Cuenta del usuario del sistema asociado con Google Authenticator.
Resultado de la terminación	1.Ingreso del usuario exitoso. 2.Pantalla de inicio de sesión.
Excepciones	1.Clave incorrecta. 1.1Volver a pedir clave.
Asociaciones de casos de uso	CDU.03
Resumen de entradas	1.Clave token de Google Autheticator.
Resumen de salidas	1.Ingreso exitoso. 2.Usuario listo para utilizar el sistema dependiendo de su nivel de accesibilidad. 3.Pantalla de inicio.

Identificación de caso de uso	CDU03
Nombre	Inicio.
Actores	Coordinador de seguridad designado, Comité de riesgos de tecnología de información, Administrador del sistema.
Descripción del caso de uso	1.El sistema muestra la interfaz de inicio. 2.El usuario CSD tiene acceso a la gestión de activos, gestión de riesgos, gestión de incidentes y reportes (CMI). 3.El usuario CDI tiene acceso a la gestión de procesos de negocio reportes (CMI y KPI). 4.El usuario ADM tiene acceso a la configuración del sistema.
Condiciones previas	1.Usuario con sesión activa. 2.Permisos de cada usuario.
Resultado de la terminación	
Excepciones	

Asociaciones de casos de uso	CDU04, CDU05, CDU06, CDU07, CDU08, CDU09, CDU10, CDU11, CDU12, CDU13, CDU14, CDU15, CDU16, CDU17, CDU18, CDU19, CDU20, CDU21, CDU22, CDU23, CDU24, CDU25, CDU25, CDU26, CDU27, CDU28, CDU29, CDU30, CDU31, CDU32, CDU33, CDU34, CDU35, CDU36, CDU37, CDU38, CDU39, CDU40, CDU41, CDU42, CDU43, CDU44, CDU45, CDU46, CDU47, CDU48, CDU49, CDU50, CDU51, CDU52, CDU53, CDU54, CDU55, CDU56, CDU57.
Resumen de entradas	
Resumen de salidas	1.Pantalla de inicio.

Identificación de caso de uso	CDU04
Nombre	Registro de activos de información de edificaciones.
Actores	Coordinador de seguridad designado
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de activos de edificación. 2.Se elige la clasificación de edificación. 3.Se elige la sub clasificación de edificación. 4.La clave de identificación de activo se genera automáticamente. 5.Ingreso de descripción. 6.Ingreso de la ubicación. 7.Ingreso de estado (Activo/Inactivo). 8.Ingreso de valoración de confidencialidad. 9.Ingreso de valoración de integridad. 10.Ingreso de valoración de disponibilidad. 11. Cálculo y visualización automática de valoración total de activo de información (valoración total, valoración escrita). 12.Cálculo de impacto de activo en dimensiones de disponibilidad, integridad, confidencialidad. 13.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de activos de información de edificaciones. 5. Valoraciones de todas las dimensiones son de 0-10.
Resultado de la terminación	1.Registro de activos de información de edificación. 2.Cálculo de impacto del activo de información en dimensiones: Integridad, Confidencialidad, Disponibilidad.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	

Resumen de entradas	1.Datos de activos de información.
Resumen de salidas	1.Información de activos de edificación guardada correctamente.

Identificación de caso de uso	CDU05
Nombre	Registro de activos de información de hardware.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de activos de hardware. 2.Se elige la clasificación de hardware. 3.Se elige la sub clasificación de hardware. 4.La clave de identificación de activo se genera automáticamente. 5.Ingreso de tipo. 6.Ingreso de número de serie. 7.Ingreso de descripción. 8.Ingreso de Dirección física. 9.Ingreso de fecha de compra. 10.Ingreso de estado (Activo/Inactivo). 11.Ingreso de valoración de integridad. 12.Ingreso de valoración de disponibilidad. 13.Ingreso de valoración de confidencialidad. 14. Cálculo y visualización automática de valoración total de activo de información (valoración total, valoración escrita). 15.Cálculo de impacto de activo en dimensiones de disponibilidad, integridad, confidencialidad. 16.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de activos de información de hardware. 5. Valoraciones de todas las dimensiones son de 0-10.
Resultado de la terminación	1.Registro de activos de información de hardware. 2.Cálculo de impacto del activo de información en dimensiones: Integridad, Confidencialidad, Disponibilidad.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de activos de información.
Resumen de salidas	1.Información de activos de hardware guardada correctamente.

Identificación de caso de uso	CDU06

Nombre	Registro de activos de información de software.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de activos de software. 2.Se elige la categoría de software. 3.Se elige la sub categoría de software. 4.La clave de identificación de activo se genera automáticamente. 5.Ingreso de descripción. 6.Ingreso de versión. 7.Ingreso de número de serie. 8.Ingreso de clave de activación. 9.Ingreso de actualización. 10.Ingreso de proveedor. 11.Ingreso de estado (Activo/Inactivo). 12.Ingreso de valoración de integridad. 13.Ingreso de valoración de disponibilidad. 14.Ingreso de valoración de confidencialidad. 15. Cálculo y visualización automática de valoración total de activo de información. 16.Cálculo de impacto de activo en dimensiones de disponibilidad, integridad, confidencialidad. 17.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de activos de información de software. 5. Valoraciones de todas las dimensiones son de 0-10.
Resultado de la terminación	1.Registro de activos de información de software. 2.Cálculo de impacto del activo de información en dimensiones: Integridad, Confidencialidad, Disponibilidad.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de activos de información.
Resumen de salidas	1.Información de activos de software guardada correctamente.

Identificación de caso de uso	CDU07
Nombre	Registro de activos de información electrónica.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de activos de información electrónica. 2.Se elige la categoría de información electrónica.

	3.La clave de identificación de activo se genera automáticamente. 4.Ingreso de descripción. 5.Ingreso de tipo. 6.Ingreso de fecha de creación. 7.Ingreso de tamaño. 8.Ingreso de permisos. 9.Ingreso de ubicación. 10.Ingreso de nombre. 11.Ingreso de fecha de modificación. 12.Ingreso de creador de la información. 13.Ingreso de estado (Activo/Inactivo). 14.Ingreso de valoración de integridad. 15.Ingreso de valoración de disponibilidad. 16.Ingreso de valoración de confidencialidad. 17. Cálculo y visualización automática de valoración total de activo de información. 18.Cálculo de impacto de activo en dimensiones de disponibilidad, integridad, confidencialidad. 19.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de activos de información de información electrónica. 5. Valoraciones de todas las dimensiones son de 0-10.
Resultado de la terminación	1.Registro de activos de información electrónica. 2.Cálculo de impacto del activo de información en dimensiones: Integridad, Confidencialidad, Disponibilidad.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de activos de información.
Resumen de salidas	1.Información de activos de información electrónica guardada correctamente.

Identificación de caso de uso	CDU08
Nombre	Registro de activos de información en papel.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de activos de información en papel. 2.Se elige la categoría de información electrónica. 3.La clave de identificación de activo se genera automáticamente. 4.Ingreso de descripción. 5.Ingreso de tipo.

	6.Ingreso de fecha de creación. 7.Ingreso de ubicación. 8.Ingreso de nombre. 9.Ingreso de fecha de modificación. 10.Ingreso de creador de la información. 11.Ingreso de estado (Activo/Inactivo). 12.Ingreso de valoración de integridad. 13.Ingreso de valoración de disponibilidad. 14.Ingreso de valoración de confidencialidad. 15. Cálculo y visualización automática de valoración total de activo de información. 16.Cálculo de impacto de activo en dimensiones de disponibilidad, integridad, confidencialidad. 17.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de activos de información en papel. 5. Valoraciones de todas las dimensiones son de 0-10.
Resultado de la terminación	1.Registro de activos de información en papel. 2.Cálculo de impacto del activo de información en dimensiones: Integridad, Confidencialidad, Disponibilidad.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de activos de información.
Resumen de salidas	1.Información de activos de información en papel guardada correctamente.

Identificación de caso de uso	CDU09
Nombre	Registro de activos de información de infraestructura de comunicaciones.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de activos de información de infraestructura de comunicaciones. 2.Se elige la categoría de infraestructura de comunicaciones. 3.La clave de identificación de activo se genera automáticamente. 4.Ingreso de tipo. 5.Ingreso de descripción. 6.Ingreso de categoría. 7.Ingreso de nombre. 8.Ingreso de proveedor. 9.Ingreso de fecha de contrato. 10.Ingreso de estado (Activo/Inactivo).

	11.Ingreso de valoración de integridad. 12.Ingreso de valoración de disponibilidad. 13.Ingreso de valoración de confidencialidad. 14. Cálculo y visualización automática de valoración total de activo de información. 15.Cálculo de impacto de activo en dimensiones de disponibilidad, integridad, confidencialidad. 16.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de activos de información de infraestructura de comunicaciones. 5. Valoraciones de todas las dimensiones son de 0-10.
Resultado de la terminación	1.Registro de activos de información de infraestructura de comunicaciones. 2.Cálculo de impacto del activo de información en dimensiones: Integridad, Confidencialidad, Disponibilidad.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de activos de información.
Resumen de salidas	1.Información de activos de información de infraestructura de comunicaciones guardada correctamente.

Identificación de caso de uso	CDU10
Nombre	Registro de activos de información de medios extraíbles.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de activos de información de medios extraíbles. 2.Se elige la categoría de medios extraíbles. 3.Se elige sub categoría de medios extraíbles. 4.La clave de identificación de activo se genera automáticamente. 5.Ingreso de tipo. 6.Ingreso de descripción. 7.Ingreso de categoría. 8.Ingreso de dirección física. 9.Ingreso de fecha de adquisición. 10.Ingreso de proveedor. 11.Ingreso de garantía. 12.Ingreso de estado (Activo/Inactivo). 13.Ingreso de valoración de integridad. 14.Ingreso de valoración de disponibilidad. 15.Ingreso de valoración de confidencialidad.

	16. Cálculo y visualización automática de valoración total de activo de información. 17.Cálculo de impacto de activo en dimensiones de disponibilidad, integridad, confidencialidad. 18.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de activos de información de medios extraíbles. 5. Valoraciones de todas las dimensiones son de 0-10.
Resultado de la terminación	1.Registro de activos de información de medios extraíbles. 2.Cálculo de impacto del activo de información en dimensiones: Integridad, Confidencialidad, Disponibilidad.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de activos de información.
Resumen de salidas	1.Información de activos de información de medios extraíbles guardada correctamente.

Identificación de caso de uso	CDU11
Nombre	Registro de activos de información de recursos humanos.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de activos de información de recursos humanos. 2.Se elige la categoría de recursos humanos. 3.Se elige sub categoría de recursos humanos. 4.La clave de identificación de activo se genera automáticamente. 5.Ingreso de descripción. 6.Ingreso de nombre. 7.Ingreso de apellido. 8.Ingreso de cargo. 9.Ingreso de género. 10.Ingreso de fecha de ingreso. 11.Ingreso de echa de salida. 12.Ingreso de estado (Activo/Inactivo). 13.Ingreso de valoración de integridad. 14.Ingreso de valoración de disponibilidad. 15.Ingreso de valoración de confidencialidad. 16. Cálculo y visualización automática de valoración total de activo de información. 17.Cálculo de impacto de activo en dimensiones de disponibilidad, integridad, confidencialidad.

	18.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de activos de información de recursos humanos. 5. Valoraciones de todas las dimensiones son de 0-10.
Resultado de la terminación	1.Registro de activos de información de recursos humanos. 2.Cálculo de impacto del activo de información en dimensiones: Integridad, Confidencialidad, Disponibilidad.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de activos de información.
Resumen de salidas	1.Información de activos de información de recursos humanos guardada correctamente.

Identificación de caso de uso	CDU12
Nombre	Consulta de activos de información.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de activos de información registrados, mediante una lista. 2.La lista muestra los campos de: categorías de activo, código de activo, descripción del activo, estado del activo 3.Posibilidad de filtrar la lista por categorías de activos. 4.Posibilidad de filtrar la lista por código de activos. 5.Posibilidad de filtrar la lista por estado de activos. 6.Posibilidad de ver detalles del activo. 7.Posibilidad de editar información del activo.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de activos de información.
Resultado de la terminación	1.Activos de información registrados en el sistema. 2.Filtros aplicados a la lista de activos de información.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	CDU13. CDU14.
Resumen de entradas	1.Consulta de lista de activos registrados a través de filtros. 1.1. Filtro de categoría de activo de información. (opcional).

	1.2. Filtro de código de activo. (opcional) 1.3. Filtro de estado de activos. (opcional)
Resumen de salidas	1.Registro de activos de información del sistema.

Identificación de caso de uso	CDU13
Nombre	Detalle de consulta de activo de información.
Actores	Coordinador de seguridad designado
Descripción del caso de uso	1.El sistema muestra la interfaz de detalles de activos de información. 2.Se muestra todos los campos del activo seleccionado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de activos de información. 5.Selección de consultar detalles de un activo en específico.
Resultado de la terminación	1.Información de activo seleccionado.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Selección en “ver detalle” de un activo de información.
Resumen de salidas	1.Información de activo seleccionado.

Identificación de caso de uso	CDU14
Nombre	Modificación de activos de información.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de activos. 2.El sistema inhabilita la opción de cambiar estado de activo en esta sección. 3.Ingreso de datos a modificar de activo. 4.Guardar cambios.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de activos de información. 5.Selección de editar un activo en específico.
Resultado de la terminación	1.Modificación de activos de información.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos.
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de activos de información 2.Selección de “editar” activo de información.
Resumen de salidas	1.Activos modificados correctamente.

Identificación de caso de uso	CDU15
Nombre	Baja/Alta de activos de información.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de activos (baja/alta de activos). 2.Búsqueda por código de activo. 3.Ingreso de fecha de modificación. 4.Se muestra información de activo (categoría, código, descripción y estado). 5.Se modifica estado de activo (activo/inactivo). 6.Ingreso de descripción de motivo de cambio. 7.Guardar. 8.El sistema guarda el historial de cambio de activo.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de activos de información (baja/alta de activos).
Resultado de la terminación	1.Modificación de estado de activos de información.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Búsqueda de activo a modificar estado. 2.Nuevo estado de activo.
Resumen de salidas	1.Activos modificados correctamente. 2.Guardado en historial de baja o alta de activos.

Identificación de caso de uso	CDU16
Nombre	Consulta de historial de Baja/Alta de activos de información.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de historial de activos (baja/alta de activos), y muestra la misma a través de una lista. 2.Posibilidad de filtrar la lista por código de activo. 3.Posibilidad de filtrar la lista por fecha de modificación. 4.Se muestra una lista de historial de alta/baja de activos muestra los campos de categoría, código de activo, descripción de activo, estado modificado, fecha de cambio, descripción de motivo de cambio de estado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de historial de alta/baja de activos.
Resultado de la terminación	1.Registro de historial de alta/baja de activos.
Excepciones	1.Datos no encontrados.

	1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de lista de historial de baja/alta de activos registrados a través de filtros. 1.1. Filtro de código de riesgo. (opcional). 1.2. Filtro de fecha de modificación de activos. (opcional).
Resumen de salidas	Registro de historial de baja/alta de activos.

Identificación de caso de uso	CDU17
Nombre	Registro de riegos.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de riesgos. 2.Elegir categoría de amenaza del riesgo a registrar. 3.El sistema muestra a los tipos de activos que afecta la amenaza escogida. 4.El sistema muestra las dimensiones que afecta la amenaza escogida. 5. El sistema muestra la descripción de la amenaza escogida. 6.El sistema genera un código de riesgo según la amenaza elegida. 7. Ingreso de descripción del riesgo. 8.Agregar activos de información que afecte el riesgo. 9.Quitar activos de información de selección. 10.Ingreso de número de incidentes del riesgo o ingreso de porcentaje de probabilidad de que ocurra el riesgo. 11.Ingreso de estado de riesgo (Activo/Inactivo). 12.Guardar información. 13.El sistema califica la probabilidad. 14.El sistema calcula el riesgo absoluto de los activos con respecto al riego, únicamente de las dimensiones en que afecta el riesgo. 15.Cálculo de riesgo absoluto. 16.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de riesgos.
Resultado de la terminación	1. Registro de riesgos. 2. Cálculo de riesgo acumulado. 3. Cálculo de riesgo absoluto.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	CDU18
Resumen de entradas	1.Datos de registro de riesgos

Resumen de salidas	1.Registro de riesgos guardadas correctamente. 2.Cálculo y almacenamiento riesgo acumulado de activos con respecto al riesgo. 3. Cálculo y almacenamiento de riesgo absoluto de activos de con respecto al riesgo.

Identificación de caso de uso	CDU18
Nombre	Agregar activos a registro de riesgos.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de búsqueda de activos para agregar a riesgos. 2.Se muestra una lista con los siguientes campos categoría, código de activo, descripción. 3.La lista tiene la opción se seleccionar varios activos. 4.Posibilidad de filtrar la lista por código de activo. 5.Posibilidad de filtrar la lista por categoría. 6.Agregar activo.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos lectura de datos. 4.Pantalla de consulta de activos. 5.Únicamente se muestran activos de información en estado activo. 6.Únicamente se muestran activos que tengan relación con los tipos de activos que afectan la categoría de amenaza que se está registrando.
Resultado de la terminación	1.Activo/s agregados a riesgos.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de activos registrados a través de filtros. 1.1. Filtro de código de activo de información. (opcional). 1.2. Filtro de categoría de activo. (opcional). 2. Selección de activo/s para agregar a registro de riesgos.
Resumen de salidas	1.Activos agregados correctamente a riesgos.

Identificación de caso de uso	CDU19
Nombre	Activo con relación al riesgo.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de relación de activos con riesgos. 2. Se muestra una lista con los siguientes campos código de activo, descripción de activo, valor para activo y

	riesgo (disponibilidad, confidencialidad, integridad y total), código de riesgo, descripción del riesgo, frecuencia, impacto (disponibilidad, confidencialidad e integridad), riesgo acumulado (disponibilidad, confidencialidad e integridad), riesgo absoluto y tratamiento. 3.Posibilidad de filtrar la lista por código de activo. 4.Posibilidad de filtrar la lista por código de riesgo. 5.Si el riesgo del activo no tiene un plan de tratamiento, el sistema muestra la opción de definir un plan. 6.Si el riesgo del activo tiene definido un plan de tratamiento el sistema muestra la opción de "ver detalle del plan", "editar plan" e "imprimir plan". 7. Los campos de impacto, riesgo absoluto y riesgo acumulado se los representa con los colores dados en las matrices de Ecu@Risk.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos lectura de datos. 4.Pantalla de consulta de activos con relación al riesgo. 5.Únicamente se muestran activos de información en estado activo. 6.Únicamente se muestran riesgos que estén es estado de activo.
Resultado de la terminación	1.Activos relacionados con riesgos.
Excepciones	
Asociaciones de casos de uso	CDU20. CDU21. CDU22. CDU24.
Resumen de entradas	1.Consulta de activos con relación a sus riesgos a través de filtros. 1.1. Filtro de código de activo de información. (opcional). 1.2. Filtro de código de riesgo. (opcional).
Resumen de salidas	1.Activos con todos sus riesgos. 2.Riesgos definidos y no definidos con planes de tratamiento. 3. Campos representados con colores.

Identificación de caso de uso	CDU20
Nombre	Registrar plan de tratamiento al riesgo.
Actores	Coordinador de seguridad designado.

Descripción del caso de uso	1.El sistema muestra la interfaz de registro de tratamiento de riesgos. 2.El sistema muestra el riesgo que va a mitigar el plan. 3.Elegir el tipo del plan de tratamiento. (Tratamiento específico o procedimiento normalizado) 4.Elegir el objetivo del plan de tratamiento. (Eliminar riesgo, reducir probabilidad, reducir consecuencia, prevenir riesgo, transferir riesgo, aceptar riesgo) 5.Ingresar el origen de riesgo. 6.Ingresar qué busca el plan de control. 7.El sistema genera automáticamente el código del tratamiento. 8.Ingresar el nombre de la contramedida. 9.Ingresar la descripción de la contramedida. 10.Ingresar el presupuesto para la implementación de la contramedida. 11.Ingresar la inversión real para la implementación de la contramedida. 12.Ingresar el número de semanas que se tardará en la implementación de la contramedida. 13.Ingresar la fecha de implementación de la contramedida. 14.El sistema muestra una lista con los siguientes campos: actividades, responsables, semana. En los cuales se agrega o se quita las actividades, cuáles son los responsables y el número de semana en el cual se desarrollará la implementación. 15.Ingreso de la fecha en que se realizará la medición del tratamiento con respecto al riesgo. 16.Guardar. 17. El sistema guarda toda la información del plan de tratamiento conjuntamente a qué riesgo mitiga. 18.El sistema automáticamente toma como estado activo al plan de tratamiento.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos lectura de datos. 4.Pantalla de registro de plan de tratamientos. 5.Selección de “definir tratamiento”.
Resultado de la terminación	1.Registro de plan de tratamiento de riesgos.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de plan de tratamiento de riesgos. 2.Selección de “definir tratamiento”.
Resumen de salidas	1.Registro exitoso de plan de tratamiento.

Identificación de caso de uso	CDU21
Nombre	Detalle de consulta de plan de tratamiento.
Actores	Coordinador de seguridad designado
Descripción del caso de uso	1.El sistema muestra la interfaz de detalles de plan de tratamiento. 2.Se muestra todos los campos del plan de tratamiento seleccionado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de plan de tratamiento. 5.Selección de consultar detalles de un tratamiento en específico.
Resultado de la terminación	1.Información de plan de tratamiento seleccionado.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Selección en “ver detalle” de un plan de tratamiento.
Resumen de salidas	1.Información de plan de tratamiento seleccionado.

Identificación de caso de uso	CDU22
Nombre	Modificación de plan de tratamiento.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de plan de tratamiento. 2.El sistema inhabilita la opción de cambiar estado de plan de tratamiento en esta sección. 3.Ingreso de datos a modificar de plan de tratamiento. 4.Guardar cambios.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de plan de tratamiento. 5.Selección de “editar” un plan de tratamiento en específico.
Resultado de la terminación	1.Modificación de plan de tratamiento.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos.
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de plan de tratamiento. 2.Selección de “editar” plan de tratamiento.
Resumen de salidas	1.Plan de tratamiento modificado correctamente.

Identificación de caso de uso	CDU23
Nombre	Imprimir plan de tratamiento.

Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema imprime el plan de tratamiento elegido.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Selección de "imprimir" plan de tratamiento en específico.
Resultado de la terminación	1.Impresión de plan de tratamiento.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de plan de tratamiento. 2.Selección de "imprimir" plan de tratamiento.
Resumen de salidas	1.Plan de tratamiento impreso correctamente.

Identificación de caso de uso	CDU24
Nombre	Consulta de riesgos.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de riesgos registrados, mediante una lista. 2.La lista muestra los campos de: Categorías de riesgo, código de riesgo, descripción del riesgo, estado del riesgo. 3.Posibilidad de filtrar la lista por categorías de riesgo. 4.Posibilidad de filtrar la lista por código de riesgo. 5.Posibilidad de filtrar la lista por estado de riesgo. 6.Posibilidad de ver detalles del riesgo. 7.Posibilidad de editar información del riesgo.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de riesgos registrados.
Resultado de la terminación	1.Riesgos registrados en el sistema. 2.Filtros aplicados a la lista de riesgos de información.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	CDU25. CDU26.
Resumen de entradas	1.Consulta de lista de riesgos registrados a través de filtros. 1.1. Filtro de categoría de riesgo. (opcional). 1.2. Filtro de código de riesgo. (opcional) 1.3. Filtro de estado de riesgo. (opcional)
Resumen de salidas	1.Registro de riesgos del sistema.

Identificación de caso de uso	CDU25

Nombre	Detalle de consulta de riesgos.
Actores	Coordinador de seguridad designado
Descripción del caso de uso	1.El sistema muestra la interfaz de detalles de riesgos de información. 2.Se muestra todos los campos del riesgo seleccionado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de riesgos. 5.Selección de consultar detalles de un riesgo en específico.
Resultado de la terminación	1.Información de riesgo seleccionado.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Selección en “ver detalle” de un riesgo.
Resumen de salidas	1.Información de riesgo seleccionado.

Identificación de caso de uso	CDU26
Nombre	Modificación de riesgos.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de riesgos. 2.El sistema inhabilita la opción de cambiar estado de riesgo en esta sección. 3.Ingreso de datos a modificar de riesgo. 4.Guardar cambios.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de riesgos. 5.Selección de editar un riesgo en específico.
Resultado de la terminación	1.Modificación de riesgos de información.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos.
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de riesgos. 2.Selección de “editar” riesgos.
Resumen de salidas	1.Riesgos modificados correctamente.

Identificación de caso de uso	CDU27
Nombre	Consulta de plan de tratamientos.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de planes de tratamiento registrados, mediante una lista.

	2.La lista muestra los campos de: código de plan de tratamiento, nombre del plan de tratamiento, descripción del plan de tratamiento, tipo de tratamiento, objetivo de tratamiento, fecha de medición, última medición realizada y medición. 3.Posibilidad de filtrar la lista por categorías de nombre de tratamiento. 4.Posibilidad de filtrar la lista por código de tratamiento. 5.Posibilidad de filtrar la lista por descripción de tratamiento. 6.En el campo de medición el sistema habilitará la opción de medición si la fecha para la medición se ha cumplido, caso contrario inhabilitará. 7.Posibilidad de ver detalles del plan de tratamiento. 8.Posibilidad de editar información de plan de tratamiento. 9.Posibilidad de imprimir plan de tratamiento. 10.Posibilidad de medir plan de tratamiento. 11.Posibilidad de filtrar la lista por los tratamientos que se pueden medir.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de planes de tratamiento registrados.
Resultado de la terminación	1.Planes de tratamiento registrados en el sistema. 2.Filtros aplicados a la lista de planes de tratamiento.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	CDU21. CDU22. CDU23. CDU28.
Resumen de entradas	1.Consulta de lista de activos registrados a través de filtros. 1.1. Filtro de categoría de plan de tratamiento. (opcional). 1.2. Filtro de código de tratamiento. (opcional) 1.3. Filtro de descripción de tratamiento. (opcional) 1.4. Filtro de medición de contramedidas.
Resumen de salidas	1.Tratamientos a riesgos registrados en el sistema.

Identificación de caso de uso	CDU28
Nombre	Medición plan de tratamiento.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de medición de riesgos.

	2.El sistema muestra el riesgo al que el plan de tratamiento mitiga. 3.El sistema indica todos los activos y el riesgo absoluto de cada uno. (en relación con el riesgo que los afecta) 4.Ingreso de número de incidentes o probabilidad que se materialice el riesgo aún con la implementación de contramedida. 5.Ingresar fecha de próxima medición que se realizará. 6.El sistema realiza el cálculo del riesgo residual. 7.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de medición de plan de tratamiento. 5.Selección de medición de un plan de tratamiento en específico.
Resultado de la terminación	1.Medición de plan de tratamiento.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos.
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de riesgos. 2.Selección de “medir” plan de tratamiento.
Resumen de salidas	1.Plan de tratamiento modificado correctamente.

Identificación de caso de uso	CDU29
Nombre	Activo con relación a riesgos y planes de tratamiento.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de relación de activos, riesgos y planes de tratamiento. 2.Se muestra una lista con los siguientes campos código de activo, descripción de activo, valor para activo y riesgo (disponibilidad, confidencialidad, integridad y total), código de amenaza, frecuencia, impacto (disponibilidad, confidencialidad e integridad), riesgo acumulado (disponibilidad, confidencialidad e integridad), riesgo absoluto, código de contramedida ,frecuencia de contramedida, impacto (disponibilidad, confidencialidad e integridad), riesgo residual (disponibilidad, confidencialidad e integridad), riesgo residual total. 3.Posibilidad de filtrar la lista por código de activo. 4.Posibilidad de filtrar la lista por código de tratamiento. 5.Posibilidad de filtrar la lista por código de riesgo. 6.El sistema representa los riesgos absolutos y residuales con colores según el nivel de riesgo (metodología Ecu@Risk).

Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos lectura de datos. 4.Pantalla de consulta de activos con relación al riesgo. 5.Únicamente se muestran activos de información en estado activo. 6.Únicamente se muestran riesgos que estén es estado de activo.
Resultado de la terminación	1.Activos relacionados con riesgos y tratamientos. 2.Se representan con colores según el nivel de riesgo.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de activos con relación a sus riesgos a través de filtros. 1.1. Filtro de código de activo de información. (opcional). 1.2. Filtro de código de riesgo. (opcional). 1.3. Filtro de código de tratamiento. (opcional).
Resumen de salidas	1.Activos con todos sus riesgos y tratamientos. 2.Riesgos representados con colores según su nivel.

Identificación de caso de uso	CDU30
Nombre	Baja/Alta de riesgos.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de riesgos (baja/alta de riesgos). 2.Búsqueda por código de riesgos. 3.Ingreso de fecha de modificación. 4.Se muestra información de riesgo (categoría, código, descripción y estado). 5.Se modifica estado de riesgo (activo/inactivo). 6.Ingreso de descripción de motivo de cambio. 7.Guardar. 8.El sistema guarda el historial de cambio de riesgo. 9.El riesgo cambia su estado de visualización con activos y planes de tratamiento asociados.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de riesgos de información (baja/alta de riesgos).
Resultado de la terminación	1.Modificación de estado de riesgos.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Búsqueda de riesgos a modificar estado. 2.Nuevo estado de riesgo.

Resumen de salidas	1.Riesgos modificados correctamente. 2.Guardado en historial de baja o alta de riesgos.

Identificación de caso de uso	CDU31
Nombre	Consulta de historial de Baja/Alta de riesgos.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de historial de riegos (baja/alta de riesgos), y muestra la misma a través de una lista. 2.Posibilidad de filtrar la lista por código de riesgos. 3.Posibilidad de filtrar la lista por fecha de modificación. 4.Se muestra una lista de historial de alta/baja de riesgos muestra los campos de categoría, código de riesgo, descripción de riesgo, estado modificado, descripción de motivo de cambio de estado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de historial de alta/baja de riesgos.
Resultado de la terminación	1.Registro de historial de alta/baja de riesgos.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de lista de historial de baja/alta de riesgos registrados a través de filtros. 1.1. Filtro de código de riesgo. (opcional). 1.2. Filtro de fecha de modificación de riesgo. (opcional).
Resumen de salidas	Registro de historial de baja/alta de riesgos.

Identificación de caso de uso	CDU32
Nombre	Baja/Alta de plan de tratamiento.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de plan de tratamiento (baja/alta de plan de tratamiento). 2.Búsqueda por código de plan de tratamiento. 3.Ingreso de fecha de modificación. 4.Se muestra información de plan de tratamiento (categoría, código, descripción y estado). 5.Se modifica estado de plan de tratamiento (activo/inactivo). 6.Ingreso de descripción de motivo de cambio. 7.Guardar.

	8.El sistema guarda el historial de cambio de plan de tratamiento siempre y cuando el riesgo que mitiga no esté activo. 9.El plan de tratamiento cambia su estado de visualización con activos y riesgos asociados.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de planes de tratamiento (baja/alta de riesgos). 5.Riesgo que mitiga tiene que estar inactivo.
Resultado de la terminación	1.Modificación de estado de plan de tratamiento.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Búsqueda de plan de tratamiento a modificar estado. 2.Nuevo estado de plan de tratamiento.
Resumen de salidas	1. Planes de tratamiento modificados correctamente. 2.Guardado en historial de baja o alta de planes de tratamiento.

Identificación de caso de uso	CDU33
Nombre	Consulta de historial de Baja/Alta de plan de tratamiento.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de historial de plan de tratamiento (baja/alta de riesgos), y muestra la misma a través de una lista. 2.Posibilidad de filtrar la lista por código de plan de tratamiento. 3.Posibilidad de filtrar la lista por fecha de modificación. 4.Se muestra una lista de historial de alta/baja de plan de tratamiento muestra los campos de categoría, código de plan de tratamiento, descripción de procesos de negocio, estado modificado, descripción de motivo de cambio de estado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de historial de alta/baja de plan de tratamiento.
Resultado de la terminación	1.Registro de historial de alta/baja de plan de tratamiento.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de lista de historial de baja/alta de plan de tratamiento registrados a través de filtros. 1.1. Filtro de código de plan de tratamiento. (opcional).

	1.2. Filtro de fecha de modificación de plan de tratamiento. (opcional).
Resumen de salidas	Registro de historial de baja/alta de planes de tratamiento.

Identificación de caso de uso	CDU34
Nombre	Registro de incidentes.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de incidentes. 2.Elegir categoría de incidente. 3.Elegir subcategoría de incidente. 4.El sistema genera un código de incidente. 5.Ingreso de fecha de incidente. 6.Ingreso de hora de incidente. 7.Ingreso de descripción de incidente. 8.Agregar activos de información que afecte el incidente. 9.Quitar activos de información de selección. 10.Guardar información
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de incidentes.
Resultado de la terminación	1.Almacenamiento de incidentes.
Excepciones	
Asociaciones de casos de uso	CDU18.
Resumen de entradas	1.Datos de incidente.
Resumen de salidas	Registro de incidentes de la empresa.

Identificación de caso de uso	CDU35
Nombre	Consulta de incidentes.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de incidentes registrados, mediante una lista. 2.La lista muestra los campos de: código de incidente, descripción del incidente, fecha de registro, hora de registro, categoría, subcategoría, código de activos afectados, descripción de activos. 3.Posibilidad de filtrar la lista por rango de fechas. 4.Posibilidad de filtrar la lista por categoría de incidente. 5.Posibilidad de filtrar la lista por subcategoría de incidente. 6.Posibilidad de filtrar la lista por código de activo. 7.Posibilidad de ver detalles del incidente. 8.Posibilidad de editar información del incidente.
Condiciones previas	1.Usuario con sesión activa.

	2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de incidentes registrados.
Resultado de la terminación	1.Incidentes registrados en el sistema. 2.Filtros aplicados a la lista de incidentes.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	CDU36. CDU37.
Resumen de entradas	1.Consulta de lista de incidentes registrados a través de filtros. 1.1. Filtro de categoría de incidentes. (opcional). 1.2. Filtro de código de incidentes. (opcional) 1.3. Filtro de estado de incidentes. (opcional)
Resumen de salidas	1.Registro de incidentes del sistema.

Identificación de caso de uso	CDU36
Nombre	Detalle de consulta de incidentes.
Actores	Coordinador de seguridad designado
Descripción del caso de uso	1.El sistema muestra la interfaz de detalles de incidentes. 2.Se muestra todos los campos del incidente seleccionado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de incidentes. 5.Selección de consultar detalles de un incidente en específico.
Resultado de la terminación	1.Información de incidente seleccionado.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Selección en “ver detalle” de un incidente.
Resumen de salidas	1.Información de incidente seleccionado.

Identificación de caso de uso	CDU37
Nombre	Modificación de incidentes.
Actores	Coordinador de seguridad designado.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de incidentes. 2.Ingreso de datos a modificar de incidente. 3.Guardar cambios.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de incidentes.

	5.Selección de editar un incidente en específico.
Resultado de la terminación	1.Modificación de incidente.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos.
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de incidentes. 2.Selección de "editar" incidentes.
Resumen de salidas	1.Incidentes modificados correctamente.

Identificación de caso de uso	CDU38
Nombre	Registro de procesos de negocio.
Actores	Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de procesos de negocio. 2.El sistema genera un código de proceso de negocio automáticamente. 3.Ingresar nombre del proceso de negocio. 4.Ingresar descripción del proceso de negocio. 5.Agregar activos de información que conformen el proceso de negocio. 6.Quitar activos de información de selección. 7.Guardar información
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de procesos de negocio.
Resultado de la terminación	1.Almacenamiento de procesos de negocio.
Excepciones	
Asociaciones de casos de uso	CDU18.
Resumen de entradas	1.Datos de procesos de negocio.
Resumen de salidas	Registro de procesos de negocio de la empresa.

Identificación de caso de uso	CDU39
Nombre	Consulta de procesos de negocio.
Actores	Coordinador de seguridad designado, Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de procesos de negocio registrados, mediante una lista. 2.La lista muestra los campos de: código de proceso de negocio, nombre del proceso de negocio, descripción del proceso de negocio, código de activos, descripción de activos. 3.Posibilidad de filtrar la lista por código proceso de negocio.

	4.Posibilidad de filtrar la lista por nombre de proceso de negocio. 5.Posibilidad de filtrar la lista por código de activo. 6.Posibilidad de ver detalles del proceso de negocio. 7.Posibilidad de editar información del proceso de negocio.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de procesos de negocio.
Resultado de la terminación	1.Procesos de negocio registrados en el sistema. 2.Filtros aplicados a la lista de procesos de negocio.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	CDU40. CDU41.
Resumen de entradas	1.Consulta de lista de procesos de negocio registrados a través de filtros. 1.1. Filtro de código de proceso de negocio. (opcional). 1.2. Filtro de nombre de proceso de negocio. (opcional) 1.3. Filtro de código de activo. (opcional)
Resumen de salidas	1.Registro de procesos de negocio del sistema.

Identificación de caso de uso	CDU40
Nombre	Detalle de consulta de proceso de negocio.
Actores	Coordinador de seguridad designado, Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de detalles de procesos de negocio. 2.Se muestra todos los campos del proceso de negocio seleccionado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de proceso de negocio. 5.Selección de consultar detalles de un proceso de negocio en específico.
Resultado de la terminación	1.Información de proceso de negocio seleccionado.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Selección en “ver detalle” de un proceso de negocio.
Resumen de salidas	1.Información de proceso de negocio seleccionado.

Identificación de caso de uso	CDU41

Nombre	Modificación de procesos de negocio.
Actores	Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de procesos de negocio. 2.Se deshabilita la opción de cambiar de estado (activo/inactivo) al proceso de negocio. 3.Ingreso de datos a modificar de incidente. 4.Guardar cambios.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de procesos de negocio. 5.Selección de editar un proceso de negocio en específico.
Resultado de la terminación	1.Modificación de proceso de negocio.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos.
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de procesos de negocio. 2.Selección de “editar” proceso de negocio.
Resumen de salidas	1.Procesos de negocio modificados correctamente.

Identificación de caso de uso	CDU42
Nombre	Baja/Alta de procesos de negocio.
Actores	Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de procesos de negocio (baja/alta de procesos de negocio). 2.Búsqueda por código de procesos de negocio. 3.Ingreso de fecha de modificación. 4.Se muestra información de procesos de negocio (categoría, código, descripción y estado). 5.Se modifica estado de procesos de negocio (activo/inactivo). 6.Ingreso de descripción de motivo de cambio. 7.Guardar. 8.El sistema guarda el historial de cambio de procesos de negocio 9.El proceso de negocio cambia su estado de visualización.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de procesos de negocio (baja/alta de procesos de negocio).
Resultado de la terminación	1.Modificación de estado de procesos de negocio.

Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Búsqueda de procesos de negocio a modificar estado. 2.Nuevo estado de proceso de negocio.
Resumen de salidas	1.Procesos de negocio modificados correctamente. 2.Guardado en historial de baja o alta de procesos de negocio.

Identificación de caso de uso	CDU43
Nombre	Consulta de historial de Baja/Alta de procesos de negocio.
Actores	Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de historial de procesos de negocio (baja/alta de procesos de negocio), y muestra la misma a través de una lista. 2.Posibilidad de filtrar la lista por código de procesos de negocio. 3.Posibilidad de filtrar la lista por fecha de modificación. 4.Se muestra una lista de historial de alta/baja procesos de negocio muestra los campos de código de procesos de negocio, descripción de procesos de negocio, estado modificado, descripción de motivo de cambio de estado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de historial de alta/baja de procesos de negocio.
Resultado de la terminación	1.Registro de historial de alta/baja de procesos de negocio.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de lista de historial de baja/alta de procesos de negocio registrados a través de filtros. 1.1. Filtro de código de procesos de negocio. (opcional). 1.2. Filtro de fecha de modificación de procesos de negocio. (opcional).
Resumen de salidas	Registro de historial de baja/alta de procesos de negocio.

Identificación de caso de uso	CDU44
Nombre	Registro de seguimiento de procesos de negocio.
Actores	Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de seguimiento de procesos de negocio.

	2.Búsqueda de proceso de negocio por código. 3.Búsqueda de proceso de negocio por nombre. 4.El sistema genera un código de seguimiento de proceso de negocio. 5.Ingreso de fecha de seguimiento de proceso de negocio. 6.Ingreso de hora de seguimiento de proceso de negocio. 7.Ingreso de descripción de incidente de proceso de negocio. 8.Elegir estado de proceso (Detenido/Recuperado) 9.Agregar activos incidentes que afecten a los procesos de negocio. 10.Quitar incidentes de selección. 11.Guardar información. 12.El sistema registra al proceso de negocio como "afectado".
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de registro de seguimiento de procesos de negocio.
Resultado de la terminación	1.Almacenamiento de seguimiento de procesos de negocio.
Excepciones	
Asociaciones de casos de uso	CDU48.
Resumen de entradas	1.Datos de seguimiento de procesos de negocio.
Resumen de salidas	Registro de seguimiento de procesos de negocio.

Identificación de caso de uso	CDU45
Nombre	Consulta de seguimiento de procesos de negocio.
Actores	Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de seguimiento de procesos de negocio registrados, mediante una lista. 2.La lista muestra los campos de: código de seguimiento, descripción del seguimiento, fecha de registro, estado. 3.Posibilidad de filtrar la lista por rango de fechas. 4.Posibilidad de filtrar la lista por código de seguimiento. 5.Posibilidad de ver detalles del seguimiento. 6.Posibilidad de editar información del seguimiento.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de seguimientos de procesos de negocio registrados.
Resultado de la terminación	1.Seguimiento de procesos de negocio registrados en el sistema.

	2.Filtros aplicados a la lista de seguimiento de procesos de negocio.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	CDU46. CDU47.
Resumen de entradas	1.Consulta de lista de seguimiento de procesos registrados a través de filtros. 1.1. Filtro de rango de fechas. (opcional). 1.2. Filtro de código de seguimiento. (opcional)
Resumen de salidas	1.Registro de seguimiento de procesos de negocio del sistema.

Identificación de caso de uso	CDU46
Nombre	Detalle de consulta de seguimiento de procesos de negocio del sistema.
Actores	Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de detalles de seguimiento. 2.Se muestra todos los campos del seguimiento de proceso de negocio seleccionado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de seguimiento de procesos de negocio. 5.Selección de consultar detalles de un seguimiento de proceso de negocio en específico.
Resultado de la terminación	1.Información de seguimiento de proceso de negocio seleccionado.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Selección en “ver detalle” de un seguimiento de proceso de negocio.
Resumen de salidas	1.Información de proceso de negocio seleccionado.

Identificación de caso de uso	CDU47
Nombre	Modificación de seguimiento de proceso de negocio.
Actores	Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de seguimiento de procesos de negocio. 2.Ingreso de datos a modificar de seguimiento de proceso de negocio. 3.Guardar cambios.
Condiciones previas	1.Usuario con sesión activa.

	2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de seguimiento de procesos de negocio. 5.Selección de editar un seguimiento de proceso de negocio en específico.
Resultado de la terminación	1.Modificación de seguimiento de procesos de negocio.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos.
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de seguimiento de procesos de negocio. 2.Selección de "editar" seguimientos de procesos de negocio.
Resumen de salidas	1.Seguimiento de procesos de negocio modificados correctamente.

Identificación de caso de uso	CDU48
Nombre	Agregar incidentes seguimiento de procesos de negocio.
Actores	Comité de riesgo de tecnologías de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de búsqueda de incidentes para agregar a seguimiento de procesos de negocio. 2.Se muestra una lista con los siguientes campos: código de incidente, categoría, subcategoría, fecha, descripción. 3.La lista tiene la opción se seleccionar varios incidentes. 4.Posibilidad de filtrar la lista por código de incidente. 5.Posibilidad de filtrar la lista por categoría. 6.Posibilidad de filtrar la lista por subcategoría. 6.Posibilidad de filtrar la lista por fecha de registro. 7.Agregar incidente/s.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos lectura de datos. 4.Pantalla de consulta de incidentes.
Resultado de la terminación	1.Incente/s agregados a seguimiento de procesos de negocio.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de incidentes registrados a través de filtros. 1.1. Filtro de código de incidente. (opcional). 1.2. Filtro de categoría de incidente. (opcional). 1.3. Filtro de subcategoría de incidente (opcional). 1.4. Filtro de fecha de incidente (opcional).

	2. Selección de incidente/s para agregar a seguimiento de procesos de negocio.
Resumen de salidas	1.Incidentes agregados correctamente a seguimiento de procesos de negocio.

Identificación de caso de uso	CDU49
Nombre	Generar reporte CMI.
Actores	Coordinador de seguridad designado, Comité de riesgos de tecnología de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de cuadro de mando integrado. 2.Se muestra una lista con los siguientes campos: código de proceso de negocio, descripción de proceso de negocio, código de activo, descripción de activo, valor para activo y riesgo (disponibilidad, confidencialidad, integridad y total), código de amenaza, frecuencia, impacto (disponibilidad, confidencialidad e integridad), riesgo acumulado (disponibilidad, confidencialidad e integridad), riesgo absoluto, código de contramedida ,frecuencia de contramedida, impacto (disponibilidad, confidencialidad e integridad), riesgo residual (disponibilidad, confidencialidad e integridad). 3.Posibilidad de filtrar la lista por código de proceso de negocio. 4.Posibilidad de filtrar la lista por código de activo. 5.Posibilidad de filtrar la lista por código de tratamiento. 6.Posibilidad de filtrar la lista por código de riesgo. 7.El sistema representa los riesgos absolutos y residuales con colores según el nivel de riesgo (metodología Ecu@Risk).
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos lectura de datos. 4.Pantalla de consulta de CMI. 5.Únicamente se muestran activos de información en estado activo. 6.Únicamente se muestran riesgos que estén es estado de activo. 7.Únicamente se muestran los procesos de negocio activos. 8.Posibilidad de ver detalle de proceso de negocio. 9.Posibilidad de ver detalle de activo de información. 10.Posibilidad de ver detalle de riesgo. 11.Posibilidad de ver detalle de plan de tratamiento. 12.Posibilidad de imprimir informe CMI.
Resultado de la terminación	1.Cuadro de mando integrado. 2.Se representan con colores según el nivel de riesgo.

Excepciones	
Asociaciones de casos de uso	CDU13. CDU21. CDU25. CDU40.
Resumen de entradas	1.Consulta de activos con relación a sus riesgos a través de filtros. 1.1. Filtro de código de proceso de negocio. 1.1. Filtro de código de activo de información. (opcional). 1.2. Filtro de código de riesgo. (opcional). 1.3. Filtro de código de tratamiento. (opcional).
Resumen de salidas	1.Proceso de negocio con todos sus activos, incluyendo la relación de todos sus riesgos y planes de tratamientos. 2.Riesgos representados con colores según su nivel.

Identificación de caso de uso	CDU50
Nombre	Generar reporte indicadores clave de desempeño (Incidentes).
Actores	Comité de riesgos de tecnología de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de indicador clave de desempeño de incidentes. 2.La lista muestra los campos de: código de incidente, descripción del incidente, fecha de registro, hora de registro, categoría, subcategoría, código de activos afectados, descripción de activos. 3.Posibilidad de filtrar por código de incidente. 4.Posibilidad de filtrar por descripción de incidente. 5.Posibilidad de filtrar la lista por rango de fechas. 6.Posibilidad de filtrar la lista por categoría de incidente. 7.Posibilidad de filtrar la lista por subcategoría de incidente. 8.Posibilidad de filtrar la lista por código de activo. 9.El sistema indica el número de incidentes registrados. 10.Posibilidad de imprimir informe de incidentes.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de informe de incidentes registrados.
Resultado de la terminación	1.Incidentes registrados en el sistema. 2.Filtros aplicados a la lista de incidentes.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de lista de incidentes registrados a través de filtros.

	1.1. Filtro de categoría de incidentes. (opcional) 1.2. Filtro de subcategoría de incidentes. (opcional) 1.3. Filtro de código de incidentes. (opcional) 1.4. Filtro de descripción de incidentes. (opcional) 1.5. Filtro de código de activo. (opcional) 1.6. Filtro por rango de fechas. (opcional)
Resumen de salidas	1.Informe de incidentes del sistema.

Identificación de caso de uso	CDU51
Nombre	Generar reporte indicadores clave de desempeño (Planes de tratamiento).
Actores	Comité de riesgos de tecnología de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de indicador clave de desempeño de planes de tratamiento. 2.La lista muestra los campos de: código de activo, descripción de activo, código de riesgo, descripción del riesgo, valor absoluto de riesgo, código de plan de tratamiento, descripción de plan de tratamiento, valor de riesgo residual, inversión, rendimiento. 3.Criterios de evaluación para el tratamiento (el usuario coloca las condiciones en que un tratamiento se considera eficiente o no). 4.Elegir rendimiento de tratamiento (todos/eficientes/no eficientes). 5.Posibilidad de imprimir informe.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de informe de planes de tratamiento.
Resultado de la terminación	1.Planes de tratamiento registrados en el sistema. 2.Condiciones aplicados a informe.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de lista de planes de tratamiento registrados a través de condiciones. 1.1. Condición de aceptación de plan de tratamiento. (obligatorio) 1.2. Filtro de estado de planes de tratamiento. (obligatorio)
Resumen de salidas	1.Informe de planes de tratamiento.

Identificación de caso de uso	CDU52
Nombre	Generar reporte indicadores clave de desempeño (Procesos de negocio).
Actores	Comité de riesgos de tecnología de información.
Descripción del caso de uso	1.El sistema muestra la interfaz de indicador clave de desempeño de procesos de negocio. 2.La lista muestra los campos de: código de proceso de negocio, descripción de proceso de negocio, fecha de registro, estado de proceso de negocio, código de incidente, descripción de incidente. 3.Posibilidad de escoger un rango de fechas. 4.Posibilidad de filtrar proceso de negocio. 5.Posibilidad de filtrar incidente. 6.Elegir estado de procesos de negocio (recuperados/detenidos, recuperados y detenidos). 7.Posibilidad de imprimir informe.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de informe de procesos de negocio.
Resultado de la terminación	1.Seuimiento de procesos de negocio registrados en el sistema. 2.Condiciones aplicados a informe.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de lista de procesos de negocio registrados a través de condiciones. 1.1. Filtro a partir de un rango de fechas (opcional). 1.2. Filtro a partir de código de proceso de negocio (opcional). 1.3. Filtro a partir de código de incidentes (opcional). 1.4. Condición de estado de proceso de negocio. (obligatorio)
Resumen de salidas	1.Informe de procesos de negocio.

Identificación de caso de uso	CDU53
Nombre	Registro de usuarios.
Actores	Administrador del sistema.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de usuarios. 2.Ingreso de nombre. 3.Ingreso de apellido. 4.Ingreso de usuario. 5.Ingredo de e-mail. 6.Ingreso de contraseña.

	7.Elegir grupo de usuarios (Coordinador de seguridad designado, Comité de riesgos de tecnología de información o Administrador). 8.Guardar información.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Pantalla de registro de usuarios.
Resultado de la terminación	1.Registro de usuarios.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de usuario del sistema.
Resumen de salidas	1.Información de usuario guardada correctamente.

Identificación de caso de uso	CDU54
Nombre	Consulta de usuario.
Actores	Administrador del sistema.
Descripción del caso de uso	1.El sistema muestra la interfaz de consulta de usuarios registrados, mediante una lista. 2.La lista muestra los campos de: usuario, nombre, apellido, e-mail. 3.Posibilidad de filtrar la lista por nombre usuario. 4.Posibilidad de filtrar la lista por apellido. 5.Posibilidad de filtrar la lista por usuario. 6.Posibilidad de ver detalle de usuario. 7.Posibilidad de editar usuario.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de usuarios.
Resultado de la terminación	1.Usarios registrados en el sistema. 2.Filtros aplicados a la lista de usuarios.
Excepciones	1.Datos no encontrados. 1.1Mensaje que datos no se encuentran registrados.
Asociaciones de casos de uso	CDU55. CDU56.
Resumen de entradas	1.Consulta de lista de usuarios registrados a través de filtros. 1.1. Filtro de nombre de usuario. (opcional). 1.2. Filtro de apellido de usuario. (opcional) 1.3. Filtro de usuario. (opcional)
Resumen de salidas	1.Registros de usuarios del sistema.

Identificación de caso de uso	CDU55
Nombre	Detalle de consulta de usuarios.

Actores	Administrador del sistema.
Descripción del caso de uso	1.El sistema muestra la interfaz de detalles de usuarios. 2.Se muestra todos los campos del usuario seleccionado.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de consulta de usuarios. 5.Selección de consultar detalles de un usuario en específico.
Resultado de la terminación	1.Información de usuario seleccionado.
Excepciones	
Asociaciones de casos de uso	
Resumen de entradas	1.Selección en “ver detalle” de un usuario.
Resumen de salidas	1.Información de usuario seleccionado.

Identificación de caso de uso	CDU56
Nombre	Modificación de usuarios.
Actores	Administrador del sistema.
Descripción del caso de uso	1.El sistema muestra la interfaz de modificación de usuarios. 2.Ingreso de datos a modificar de usuario. 3.Guardar cambios.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de modificación de usuarios. 5.Selección de editar un usuario en específico.
Resultado de la terminación	1.Modificación de usuarios.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos.
Asociaciones de casos de uso	
Resumen de entradas	1.Datos de usuarios. 2.Selección de “editar” usuario.
Resumen de salidas	1.Usuarios modificados correctamente.

Identificación de caso de uso	CDU57
Nombre	Consulta de registro de actividades de usuarios.
Actores	Administrador del sistema.
Descripción del caso de uso	1.El sistema muestra la interfaz de registro de actividades de usuarios. 2.El sistema muestra una lista con los siguientes campos: fecha, hora, usuario, acción realizada. 3.Posibilidad de filtrar lista por fecha. 4.Posibilidad de filtrar lista por hora.

	5.Posibilidad de filtrar lista por usuario.
Condiciones previas	1.Usuario con sesión activa. 2.Usuario con permisos escritura de datos. 3.Usuario con permisos de lectura de datos. 4.Pantalla de actividades de usuarios.
Resultado de la terminación	1.Resumen de log de acciones realizadas por usuarios.
Excepciones	1.Datos incorrectos. 1.1Volver a pedir datos.
Asociaciones de casos de uso	
Resumen de entradas	1.Consulta de lista de acciones registradas a través de filtros. 1.1. Filtro de fecha. (opcional). 1.2. Filtro de hora. (opcional) 1.3. Filtro de usuario. (opcional)
Resumen de salidas	1.Registros de actividades de usuarios.

3.17. Requisitos no funcionales

El sistema debe contar con una interfaz gráfica fácil de manejar y muy intuitiva para el usuario, con explicaciones claras y concisas de cada herramienta que forman parte del sistema, esto facilitará el aprendizaje del funcionamiento y así el usuario podrá rápidamente desenvolverse y usar el sistema sin inconveniente alguno.

Se debe presentar una ventana de ayuda, en la cual el usuario podrá consultar aspectos sobre la funcionalidad de cada parte del sistema, el cálculo de los valores de riesgos, los rangos de valores que deben ingresarse, etc., es decir, una explicación clara de cómo funciona el sistema.

Se debe documentar cada parte del sistema desde su diseño hasta su implementación, con el fin de hacer que la mantenibilidad del software pueda ser más sencillo para las personas que se encarguen de hacerlo.

El sistema debe garantizar a los usuarios que la información siempre responda a los principios de seguridad: disponibilidad, integridad y confidencialidad, que no sea alterada de ninguna manera por otras personas, además, el sistema contará con un registro de actividad, el cual indicará los cambios que fueron realizados y la persona o usuario que los realizó.

Se debe garantizar la continuidad del servicio 24 horas el día los 7 días a la semana, con esquemas que permitan la recuperabilidad ante un eventual fallo del servicio en algún momento.

El diseño y arquitectura del sistema debe garantizar que registrar y consultar con grandes cantidades de datos no afecte el desempeño del software tanto en base de datos, como en tráfico de red.

Identificación del requerimiento	RNF01
Nombre	Interfaz gráfica.
Descripción	El sistema presentará una interfaz fácil de comprender y muy intuitiva para el usuario.
Prioridad	Alta

Identificación del requerimiento	RNF02
Nombre	Ayuda de manejo del sistema.
Descripción	El sistema deberá presentar una ventana de ayuda en la cual se explique el funcionamiento del mismo.
Prioridad	Alta

Identificación del requerimiento	RNF03
Nombre	Mantenimiento del sistema.
Descripción	El sistema contará con manuales de desarrollo, usuario y toda la documentación pertinente, para facilitar los mantenimientos a las personas encargadas.
Prioridad	Alta

Identificación del requerimiento	RNF04
Nombre	Seguridad de información.
Descripción	El sistema garantizará la confiabilidad de los datos almacenados por parte de los usuarios del mismo, con permisos a cada usuario.
Prioridad	Alta

Identificación del requerimiento	RNF05
Nombre	Seguimiento de actividades.
Descripción	El sistema contará con logs de registro de actividades de cada usuario, para conocer qué usuario registró, modificó o eliminó algún dato del sistema.
Prioridad	Alta

Identificación del requerimiento	RNF06
Nombre	Disponibilidad continua del sistema.
Descripción	Será un sistema que esté disponible las 24 horas del día, los 7 días de la semana, ya que es un sistema web para la carga y consulta de datos.
	Alta

Identificación del requerimiento	RNF07
Nombre	Rendimiento del sistema.
Descripción	El sistema deberá contar con un diseño y arquitectura que soporte trabajar con grandes cantidades de datos, al igual que múltiples consultas; el rendimiento del sistema no debe decaer bajo ninguna circunstancia.
	Alta

3.18. Conclusiones de la sección de levantamiento de requerimientos

La mayoría de paquetes de software de gestión de riesgos de información solamente realizan el análisis de riesgos y amenazas en los activos registrados. Lo que se plantea con el sistema Ecu@Risk es dar un valor agregado con el análisis de riesgos y amenazas de los activos de información dentro de los procesos de negocio de cada empresa, ya que es muy importante para las organizaciones conocer dónde se encuentran los riesgos e incidentes que se presentan en el desarrollo de sus actividades diarias.

En la actualidad lo que buscan los usuarios son herramientas fáciles de entender y utilizar, este es un punto muy importante dentro del diseño del sistema, ya que los esfuerzos deben estar centrados en la interfaz con el usuario la funcionalidad y la usabilidad del mismo.

La documentación del software es muy importante porque brinda la posibilidad de realizar operaciones de mantenimiento y actualizaciones de la herramienta con el mínimo esfuerzo posible, esto representa un ahorro de tiempo y dinero para las empresas.

La seguridad dentro de un sistema es un punto clave en las aplicaciones, principalmente en los softwares que están en la web porque se encuentran al alcance de todo el mundo, un sistema de esta índole debe brindar garantías a los usuarios de que sus datos estarán protegidos de ataques de personas malintencionadas que buscan dañar, robar o mal utilizar la información de las empresas.

El sistema siempre debe estar disponible en cualquier momento para su uso, el concepto de disponibilidad de servicio también hace referencia al tiempo de reparación cuando el servicio ha fallado, lo que se planifica en el sistema es que el tiempo de reparación sea el más corto luego de un fallo.

El diseño de arquitectura detrás de la aplicación debe estar siempre preparada para trabajar con grandes cantidades de datos y lista para recibir múltiples consultas y accesos, es por eso que debe contar con un buen diseño con el fin de no comprometer de ninguna manera su rendimiento, ya que un menor tiempo de latencia de respuesta del servicio significa un buen desempeño del sistema.

Con los requisitos levantados en este documento para el desarrollo del sistema Ecu@Risk se espera el diseño e implementación de un software completo de gestión de riesgos de información que ayude a las empresas MPYMES a la rápida y fácil gestión de sus activos con un costo moderado y asequible para las organizaciones.

Capítulo 4: Diseño de software

4.1. Introducción

Una vez realizada la formulación y recopilación de requisitos que debe considerar un software web para contribuir con la gestión de riesgos basado en la metodología Ecu@Risk, se debe realizar el modelado de análisis como indica García Chi (2013); el mismo que consiste en modelos de: contenido, interacción, funcional, configuración y un análisis de relación-navegación.

Como se indicó anteriormente, para la representación de los diferentes modelos se utilizará el lenguaje de modelo unificado (UML), debido a que se plantea un software orientado a objeto (DSOO), el UML es el lenguaje más indicado para interpretar los requisitos especificados en representaciones de desarrollo del software, y también permite el modelado tanto de componentes estáticos como dinámicos del software (Vidal, Schmal, Rivero, & Villaroel, 2012).

Para los autores Rumbaugh, Jacobson y Booch (2004), el diseño y modelado son muy importantes en la construcción software para:

- Comunicar de una forma óptima la estructura de un sistema.
- Detallar el comportamiento que se desea dentro del sistema.
- Ayudar a entender y comprender mejor lo que se está construyendo.
- Explorar y descubrir oportunidades de simplificación y reutilización.

Los modelos proporcionarán el diseño (los planos), para la elaboración del sistema, tanto en el punto de vista estructural (organización del sistema), como en el punto de vista de comportamiento (dinámica del sistema).

4.2. Modelo de contenido

García Chi (2013) indica que el modelo de contenido abarca los elementos estructurales de la aplicación, es decir, en este modelo encontraremos las clases de contenido que conforman a la aplicación, que se derivan del análisis gramatical de los casos de uso. Estos fueron analizados y desarrollados en el capítulo anterior.

La representación del modelo de contenido se lo realizará mediante el uso de diagramas de clase.

4.2.1. Diagramas de clase

Para el autor Kendall (2011) definir las clases de un sistema es la tarea más importante dentro de la programación orientada a objetos. La clase es una agrupación de cosas que tienen las mismas propiedades y actuar similar. Los diagramas de clase describen la estructura estática de un sistema y no muestran ningún procesamiento en especial, además indica cómo se relacionan las clases entre sí.

4.2.2. Diagrama de clases del software Ecu@Risk

A continuación, se presenta el diagrama de clases del software Ecu@Risk:

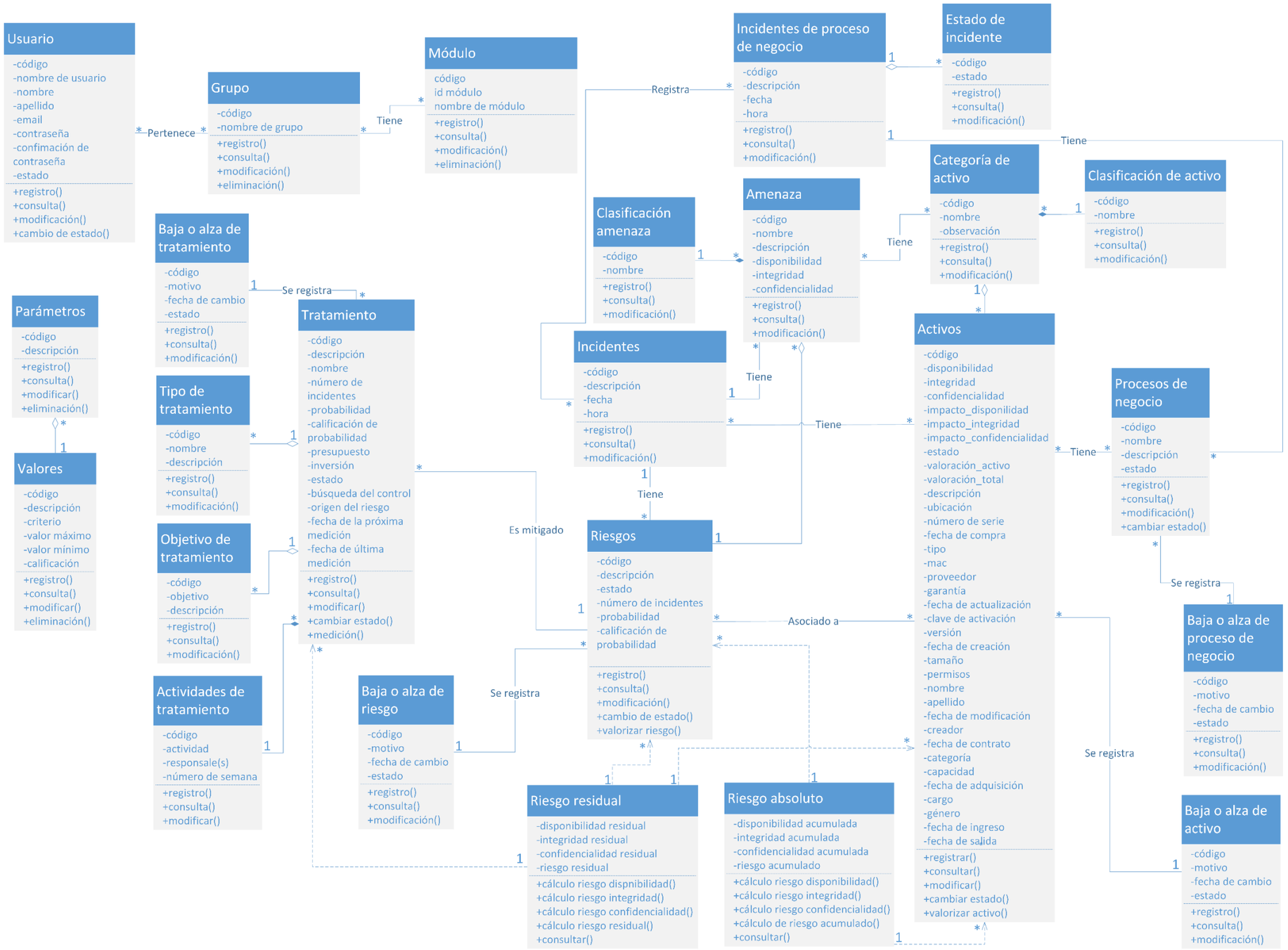

Ilustración 21: Diagrama de clases del sistema Ecu@Risk.
Fuente: Elaboración Propia.

4.3. Modelo de interacción

El modelo de interacción representa cómo interactúa el software con el usuario. Para su representación, se utilizan los diagramas de secuencia.

Los diagramas de secuencia muestran las interacciones de objetos organizadas en la secuencia de tiempo. En particular, muestra los objetos que participan en una interacción y la secuencia de mensajes intercambiados. (Rumbaugh, Jacobson, & Booch, 2004).

4.3.1. Diagramas de secuencia del software Ecu@Risk

Inicio de sesión

La ilustración 22 representa el inicio de sesión de un usuario:

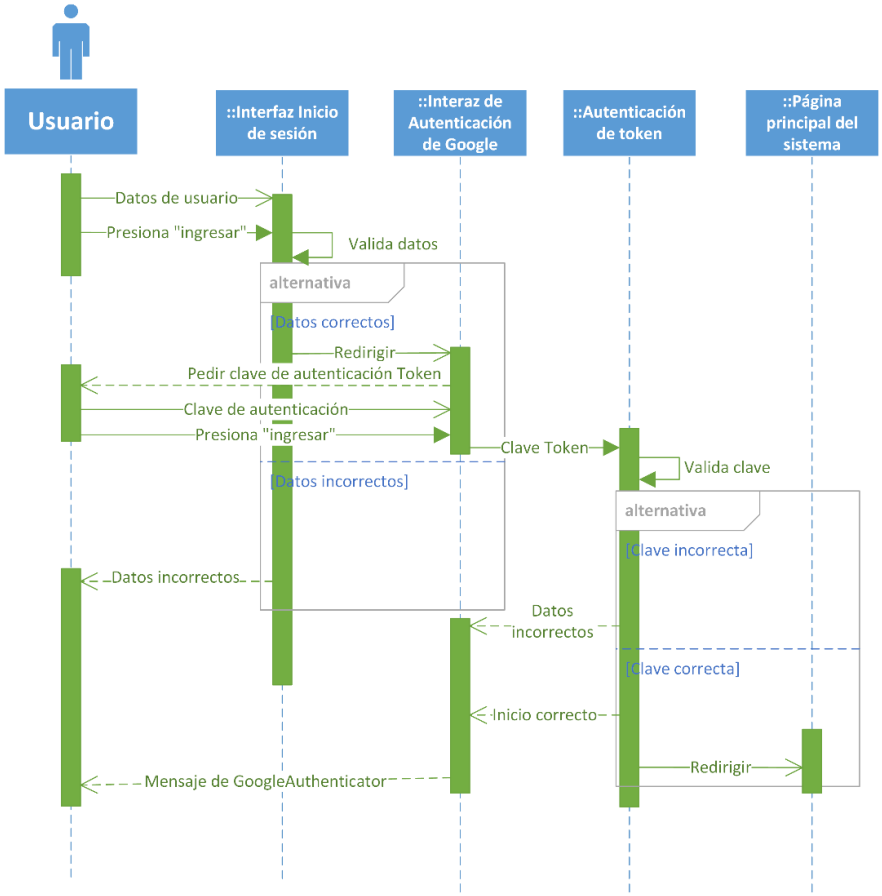

Ilustración 22: Inicio de sesión de usuario.
Fuente: Elaboración propia.

Gestión de activos

La ilustración 23 representa el registro de activos de información:

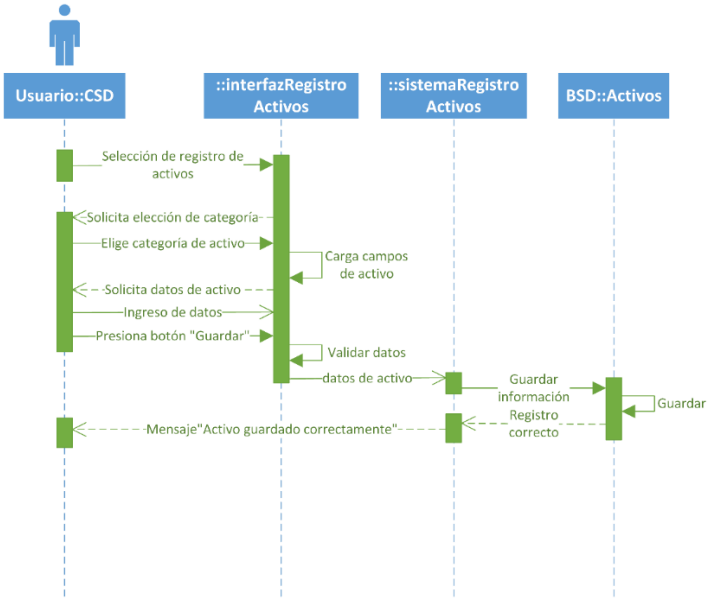

Ilustración 23: Registro de activos de información.
Fuente: Elaboración propia.

La ilustración 24 representa la consulta de activos de información registrados:

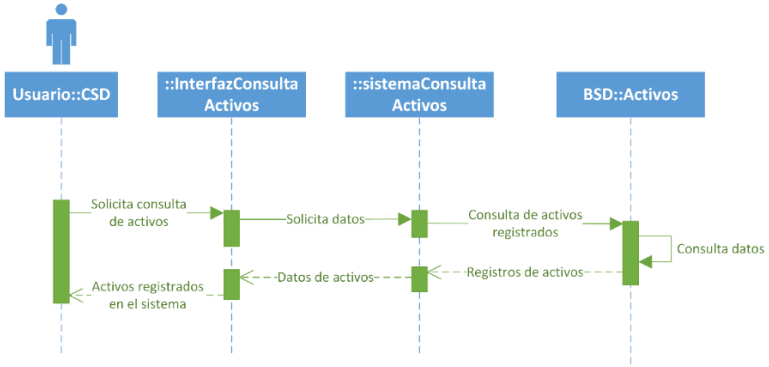

Ilustración 24: Consulta de activos de información.
Fuente: Elaboración propia.

La ilustración 25 representa la consulta individual de los detalles de cada activo de información registrado:

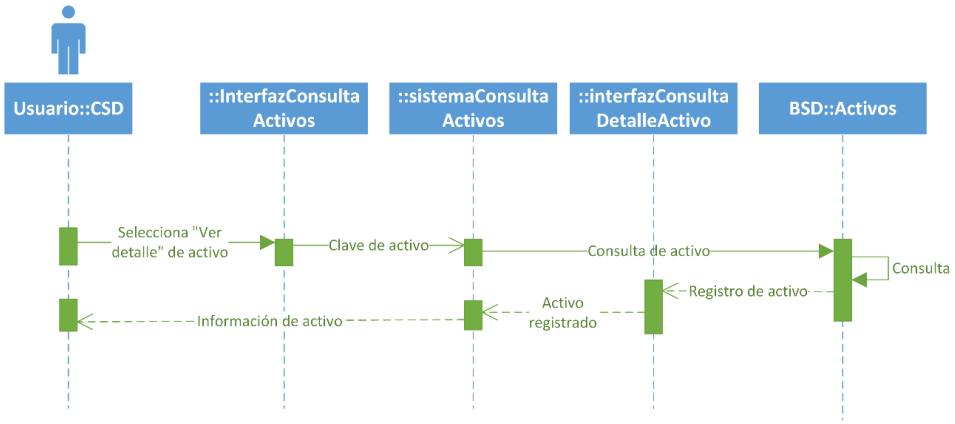

Ilustración 25: Consulta de información detallada de activo de información.
Fuente: Elaboración propia.

La ilustración 26 representa la edición de los datos de un activo de información registrado:

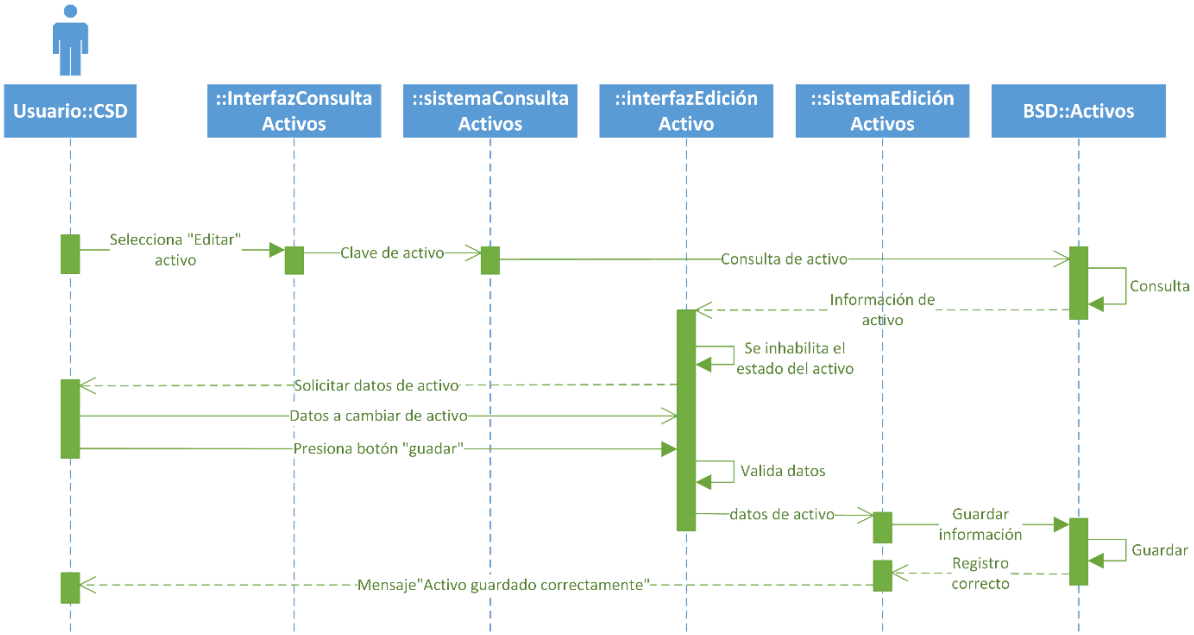

Ilustración 26: Edición de un activo de información.
Fuente: Elaboración propia.

La ilustración 27 representa el registro de un activo de información dado de baja o dado de alta en la empresa:

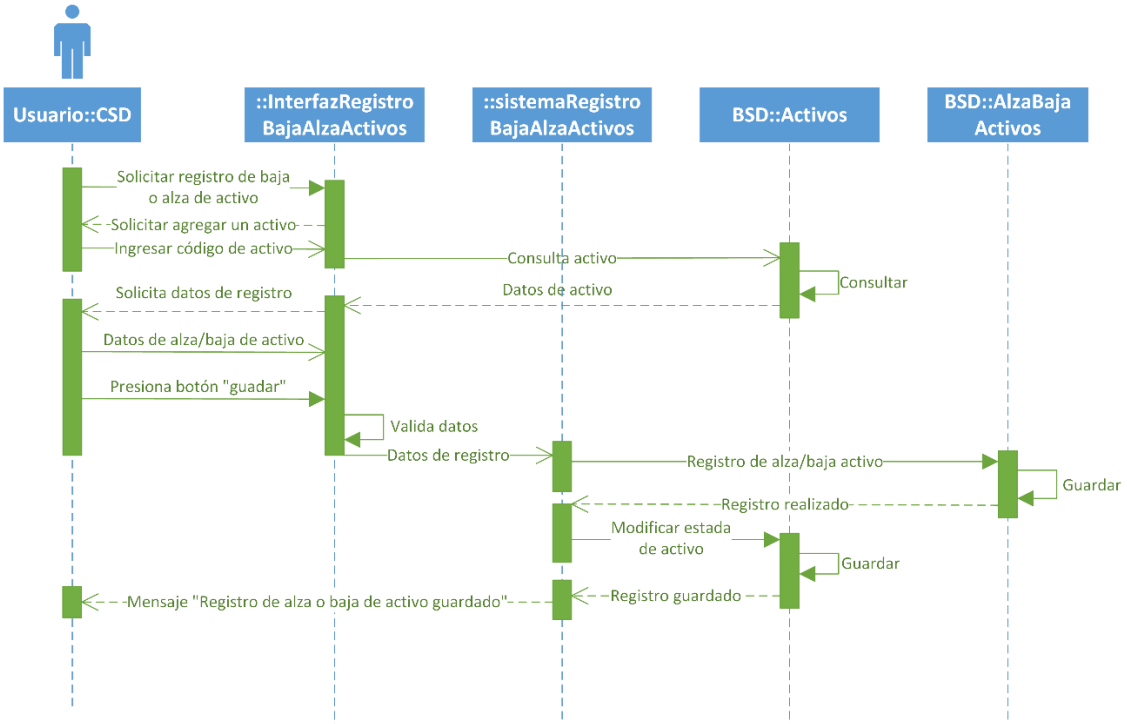

Ilustración 27: Registro de baja o alta de activo de información.
Fuente: Elaboración propia.

La ilustración 28 representa la consulta de los activos de información dados de baja o dados de alta en la empresa:

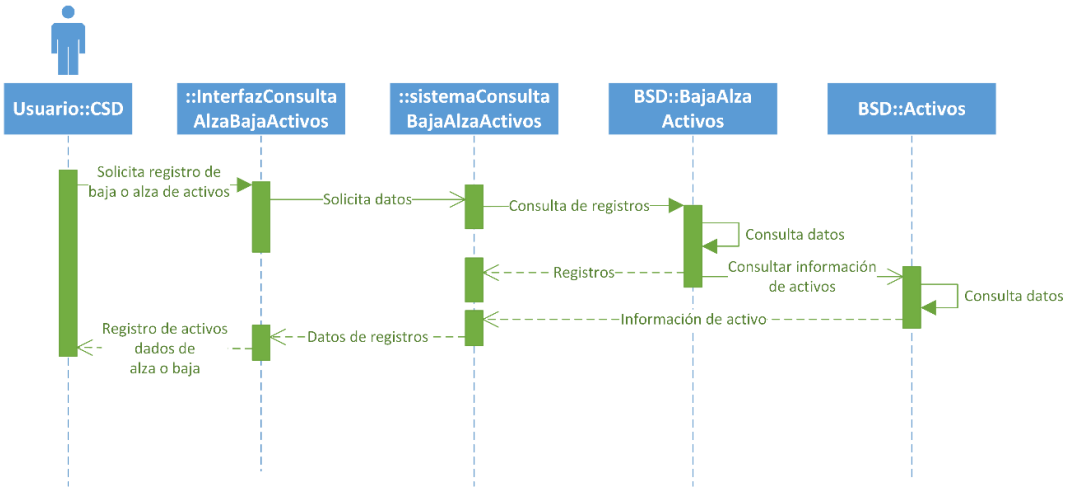

Ilustración 28: Consulta de activos dados de baja o alta.
Fuente: Elaboración propia.

Gestión de riesgos y tratamientos

La ilustración 29 representa el registro de riesgos:

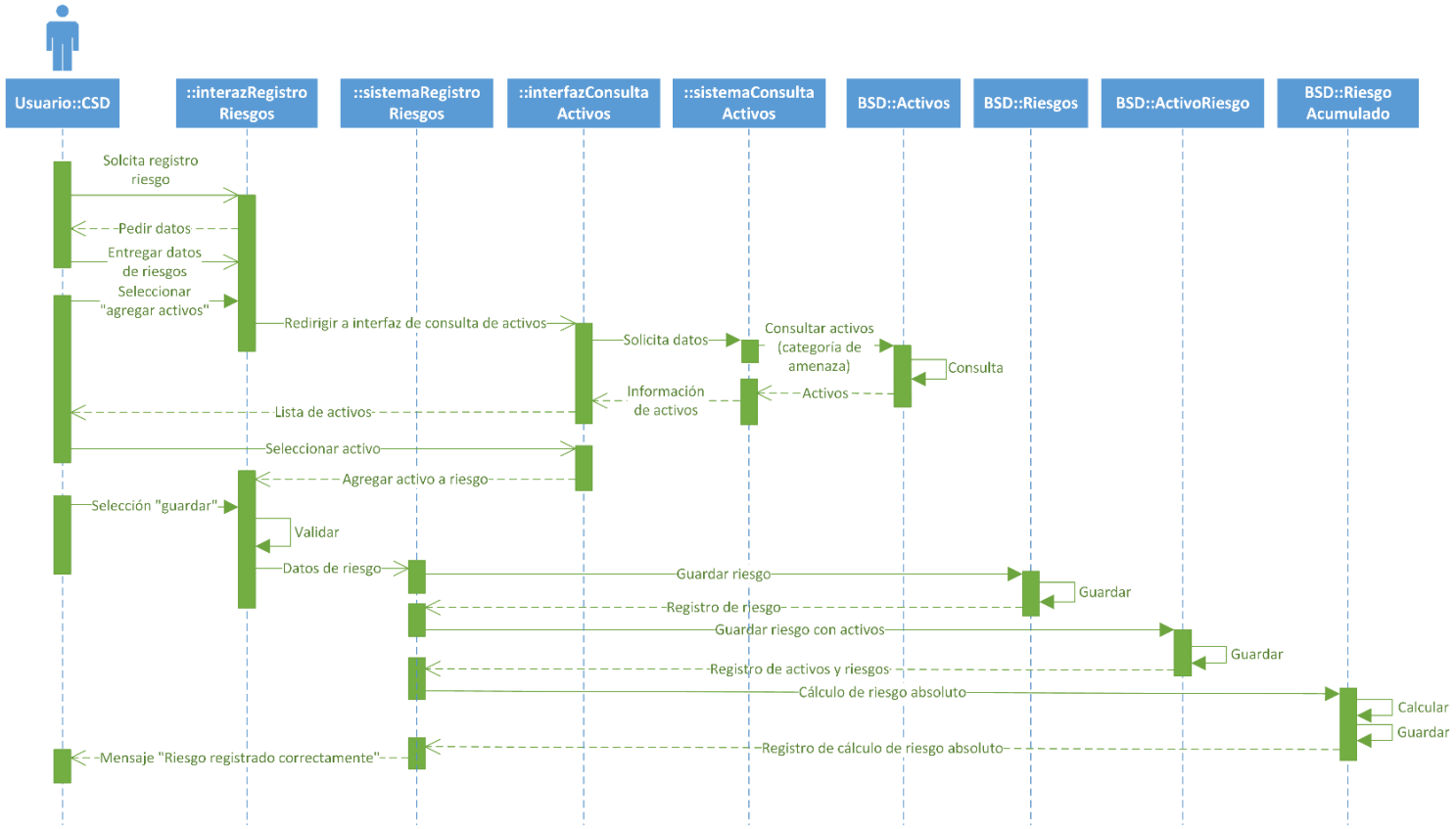

Ilustración 29: Registro de riesgos.
Fuente: Elaboración propia.

La ilustración 30 representa la consulta de riesgos registrados en el sistema:

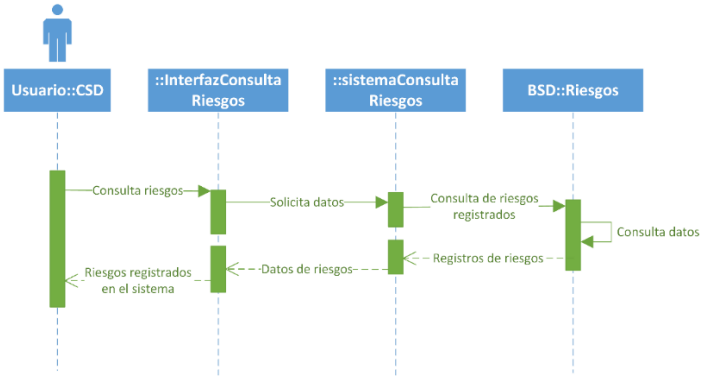

Ilustración 30: Consulta de riesgos registrados en el sistema.
Fuente: Elaboración propia.

La ilustración 31 representa la consulta de los detalles de un riesgo registrado en el sistema:

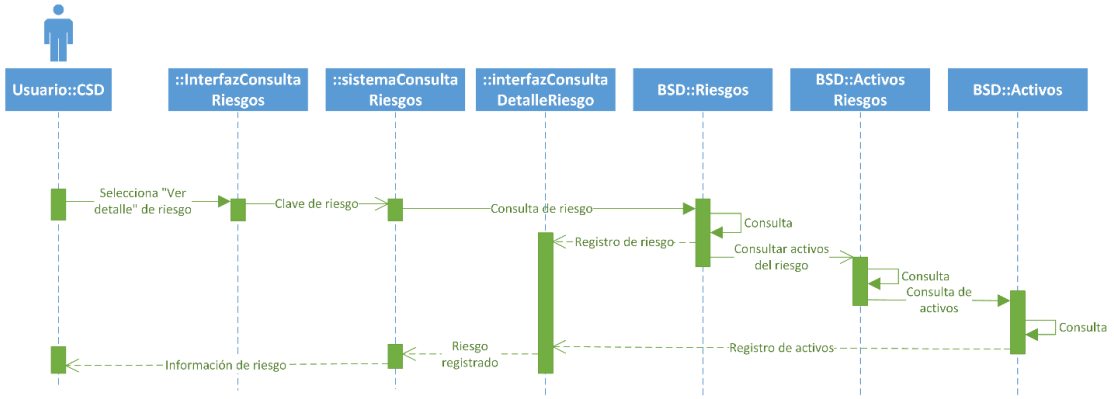

Ilustración 31: Consulta de detalles de riesgo registrado.
Fuente: Elaboración propia.

La ilustración 32 representa la edición de un riesgo registrado en el sistema:

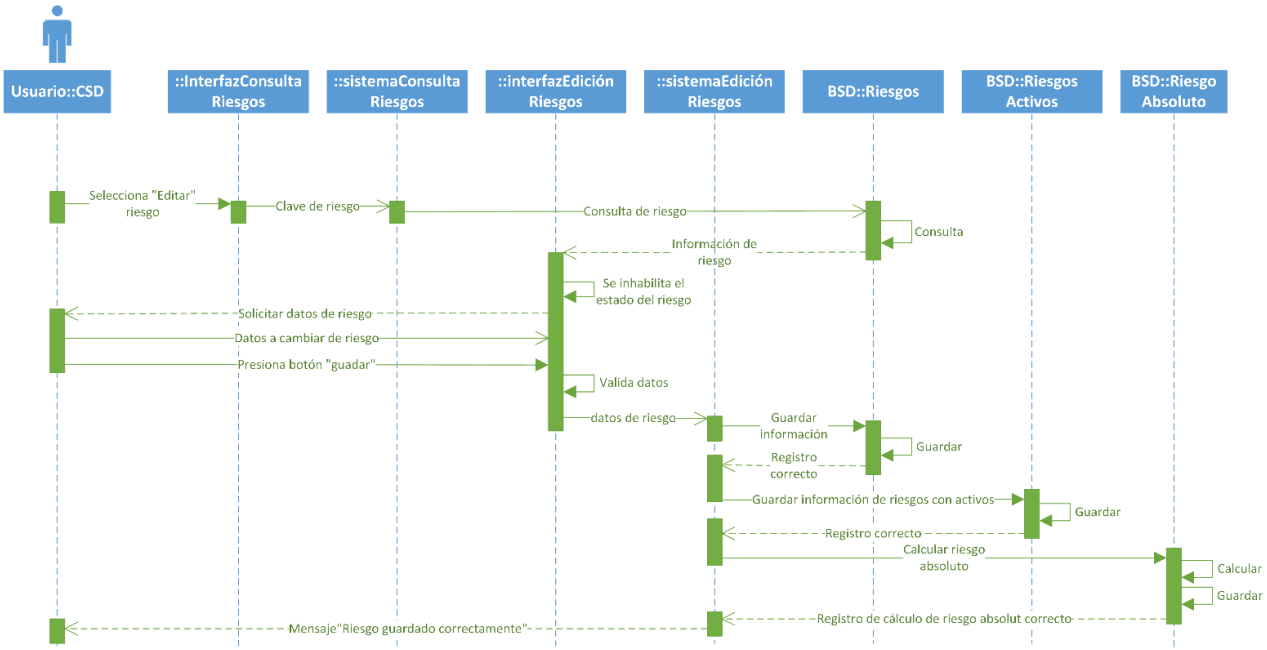

Ilustración 32: Edición de información de un riesgo.
Fuente: Elaboración propia.

La ilustración 33 representa el registro de baja de un riesgo o alta de un riesgo registrado en el sistema:

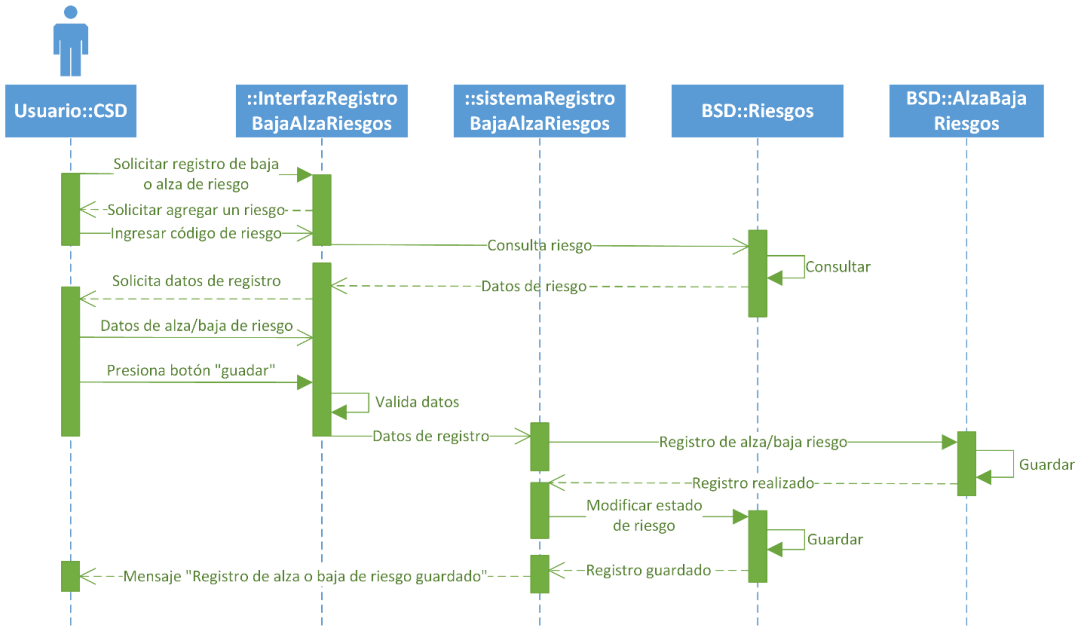

Ilustración 33: Registro de baja o alta de riesgo registrados en el sistema.
Fuente: Elaboración propia.

La ilustración 34 representa la consulta del registro de baja o alta de riesgos:

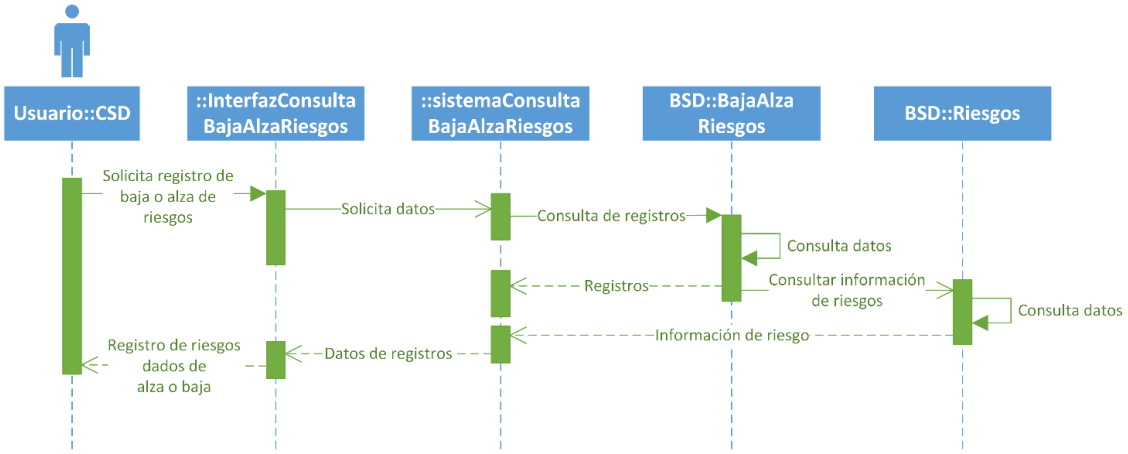

Ilustración 34:Consulta de registro de baja o alta de riesgos registrados en el sistema.
Fuente: Elaboración propia.

La ilustración 35 representa la relación entre los activos y los riesgos que afectan a cada uno de los activos registrados en el sistema, también se muestran los riesgos absolutos y acumulados:

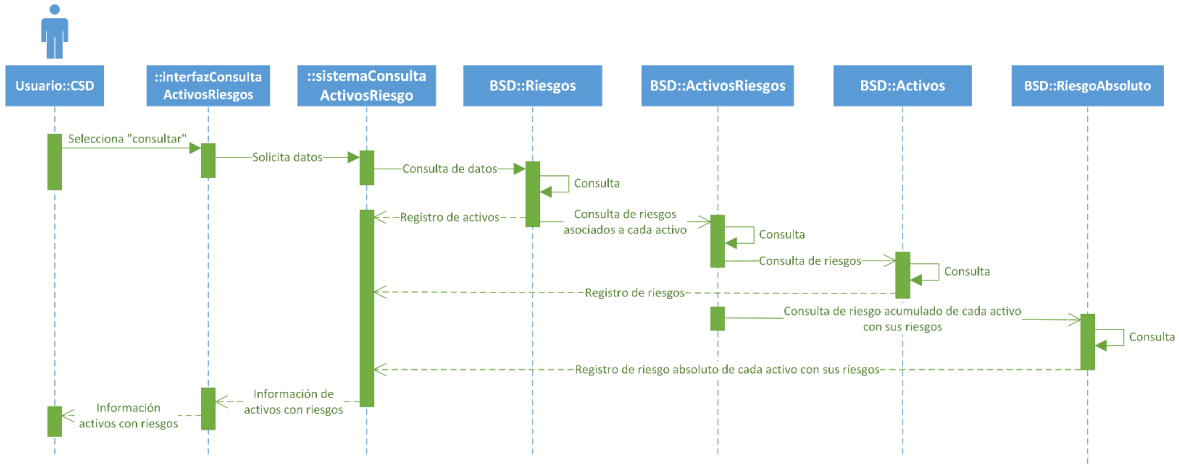

Ilustración 35: Relación entre activos y riesgos.
Fuente: Elaboración propia.

La ilustración 36 representa el registro de un plan de tratamiento que mitigue al riesgo:

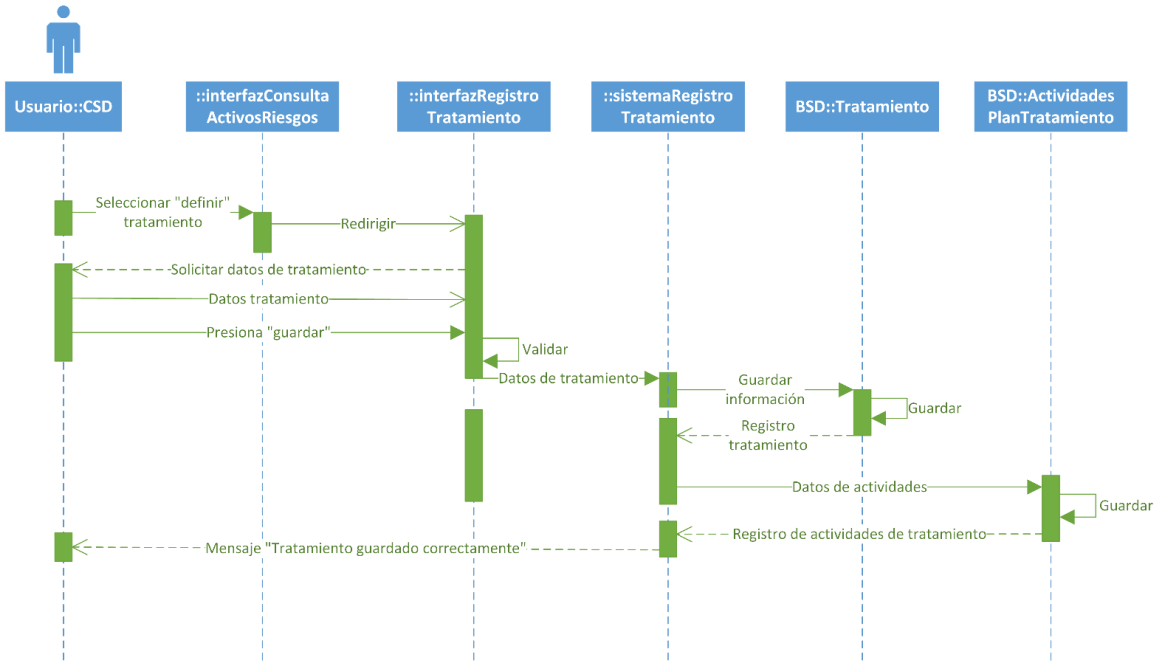

Ilustración 36: Registro de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 37 representa la consulta de los planes de tratamiento registrados en el sistema:

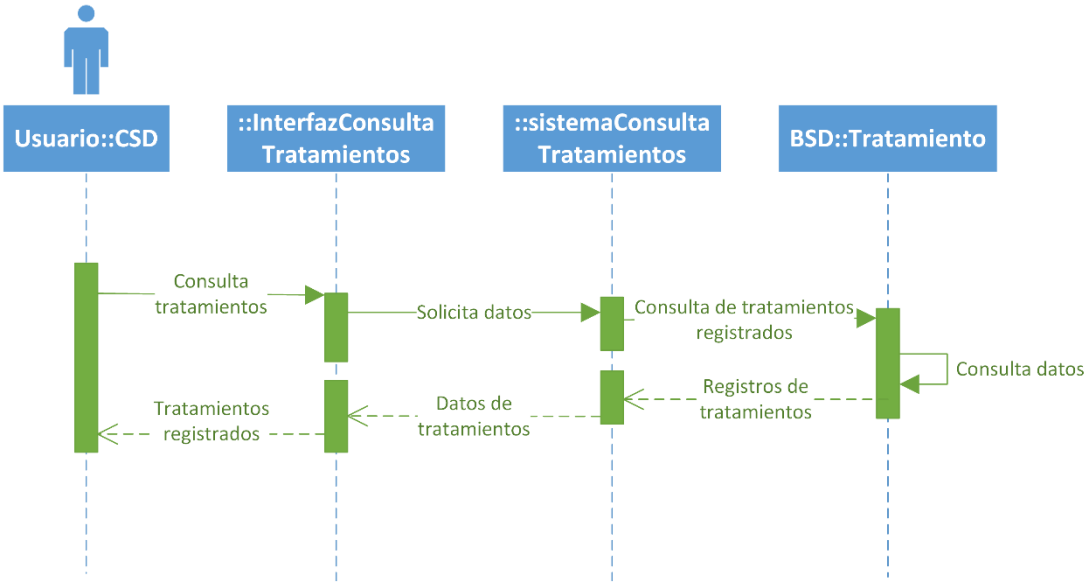

Ilustración 37: Consulta de planes de tratamiento registrados en el sistema.
Fuente: Elaboración propia.

La ilustración 38 representa la consulta de los detalles de un plan de tratamiento registrado en el sistema:

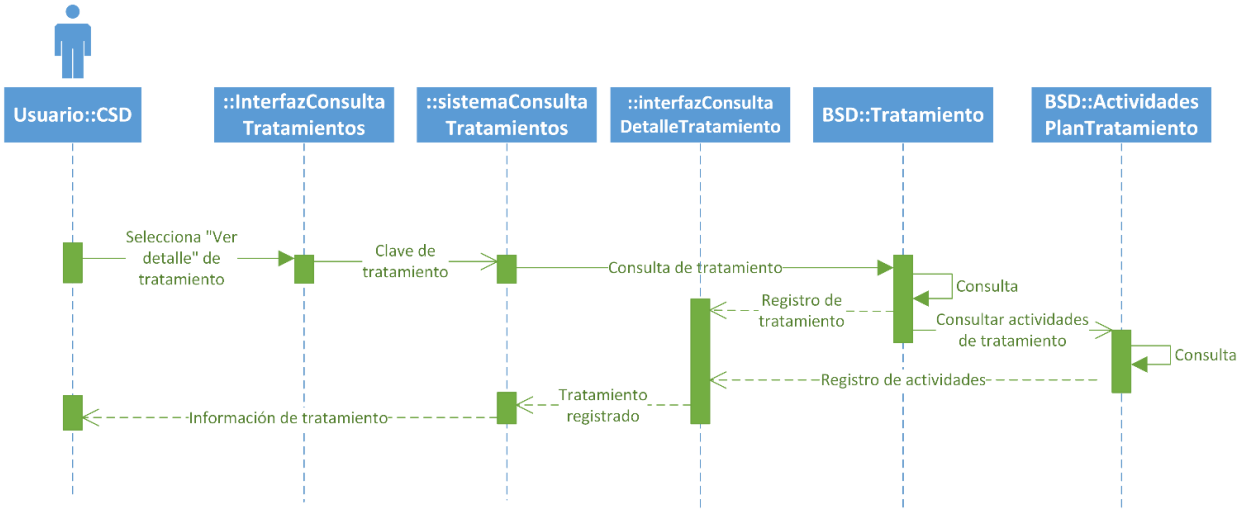

Ilustración 38:Consulta de detalles de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 39 representa la edición de información de un plan de tratamiento registrado en el sistema:

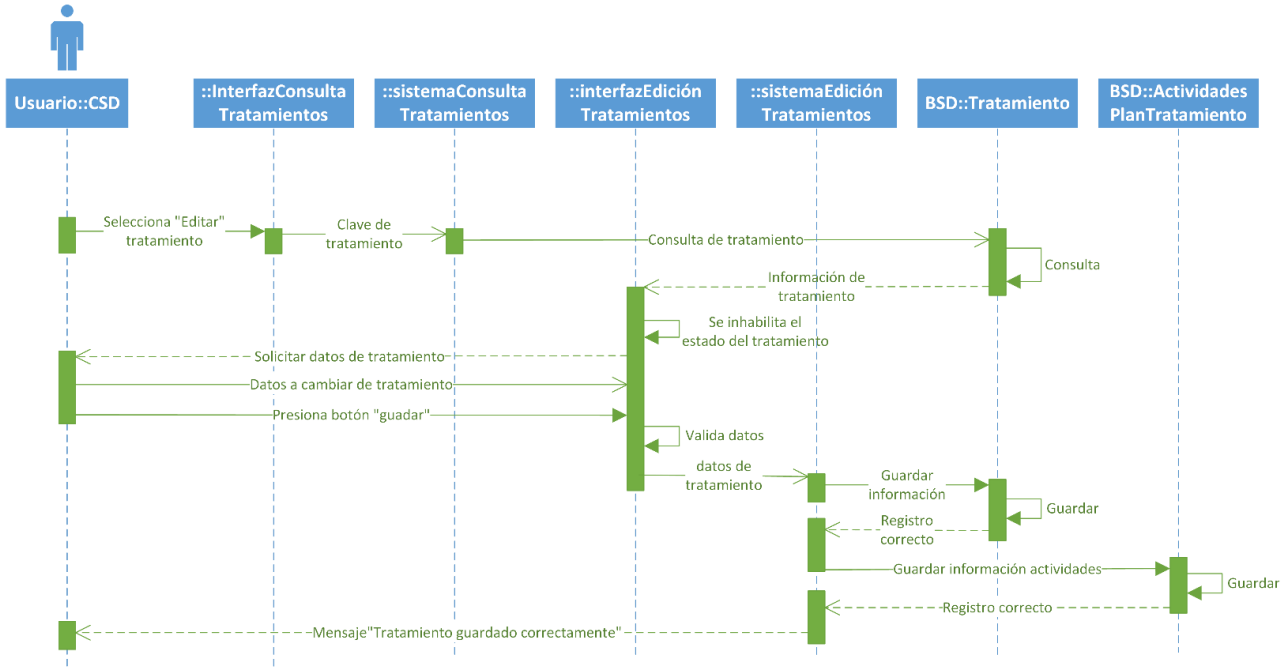

Ilustración 39: Edición de un plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 40 representa la medición y cálculo de riesgo residual de un plan de tratamiento registrado en el sistema:

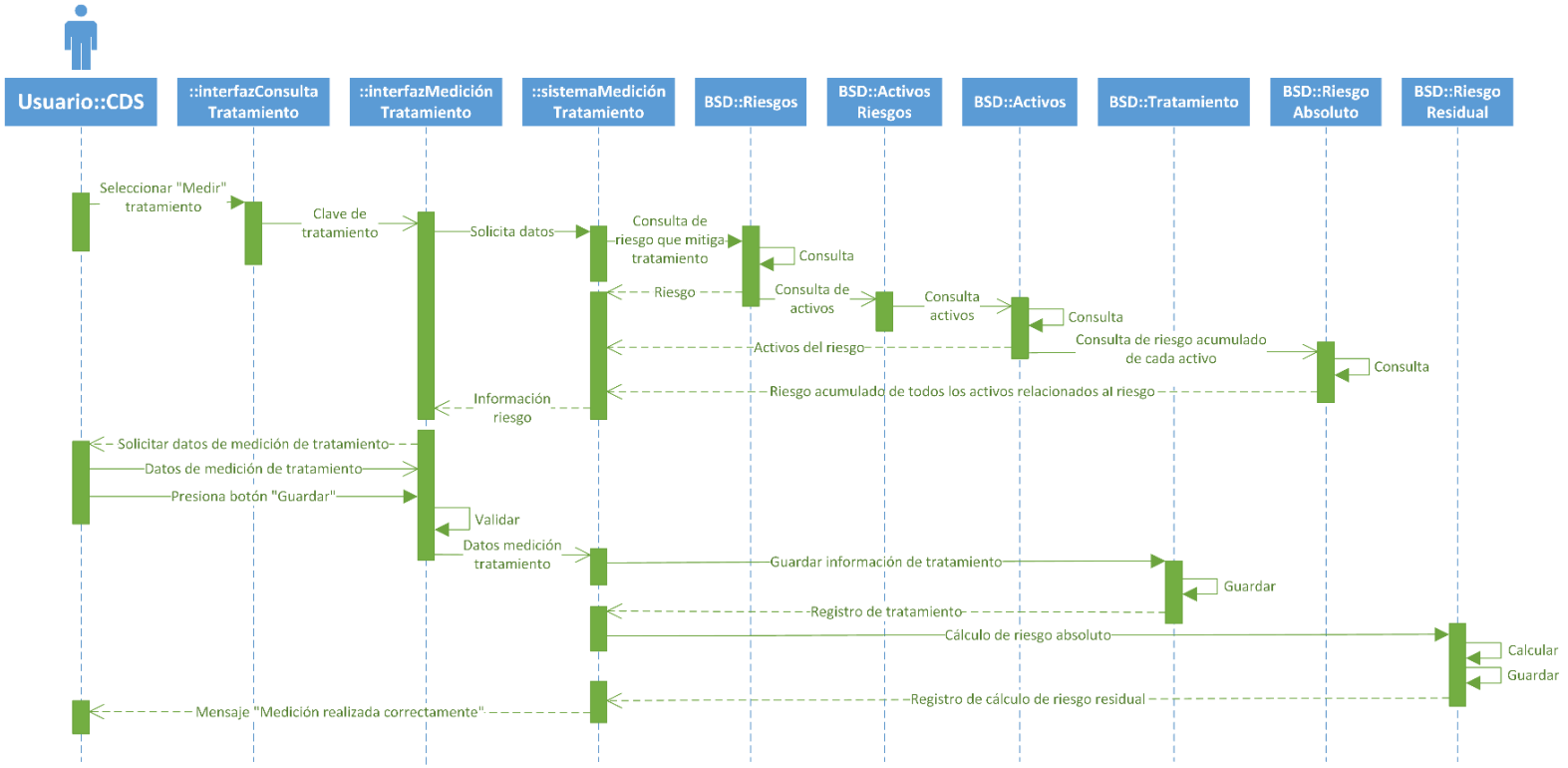

Ilustración 40: Medición de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 41 representa el registro de baja o registro de alta de un plan de tratamiento:

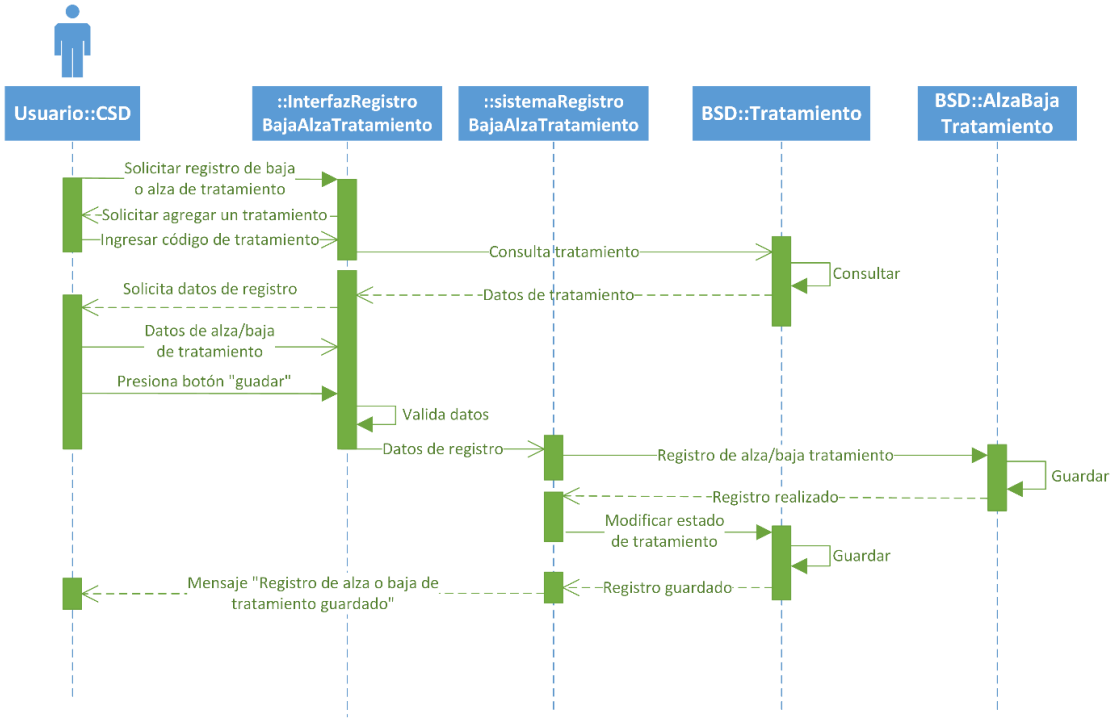

Ilustración 41: Registro de alta o baja de un plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 42 representa la consulta de registro baja o alta de un plan de tratamiento:

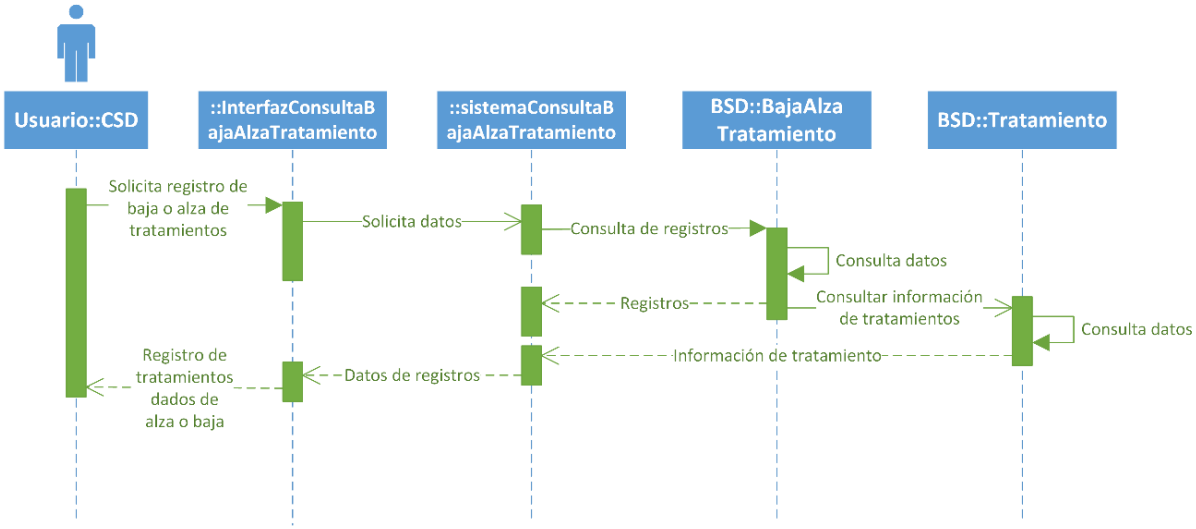

Ilustración 42: Consulta de registro de baja o alta de planes de tratamiento.
Fuente: Elaboración propia.

La ilustración 43 representa la relación entre los activos de información y cada uno de los riesgos que los atacan, también se presenta el plan de tratamiento que mitiga cada riesgo, así como, los riesgos absolutos y acumulados, finalmente se muestra los riesgos residuales de cada tratamiento.

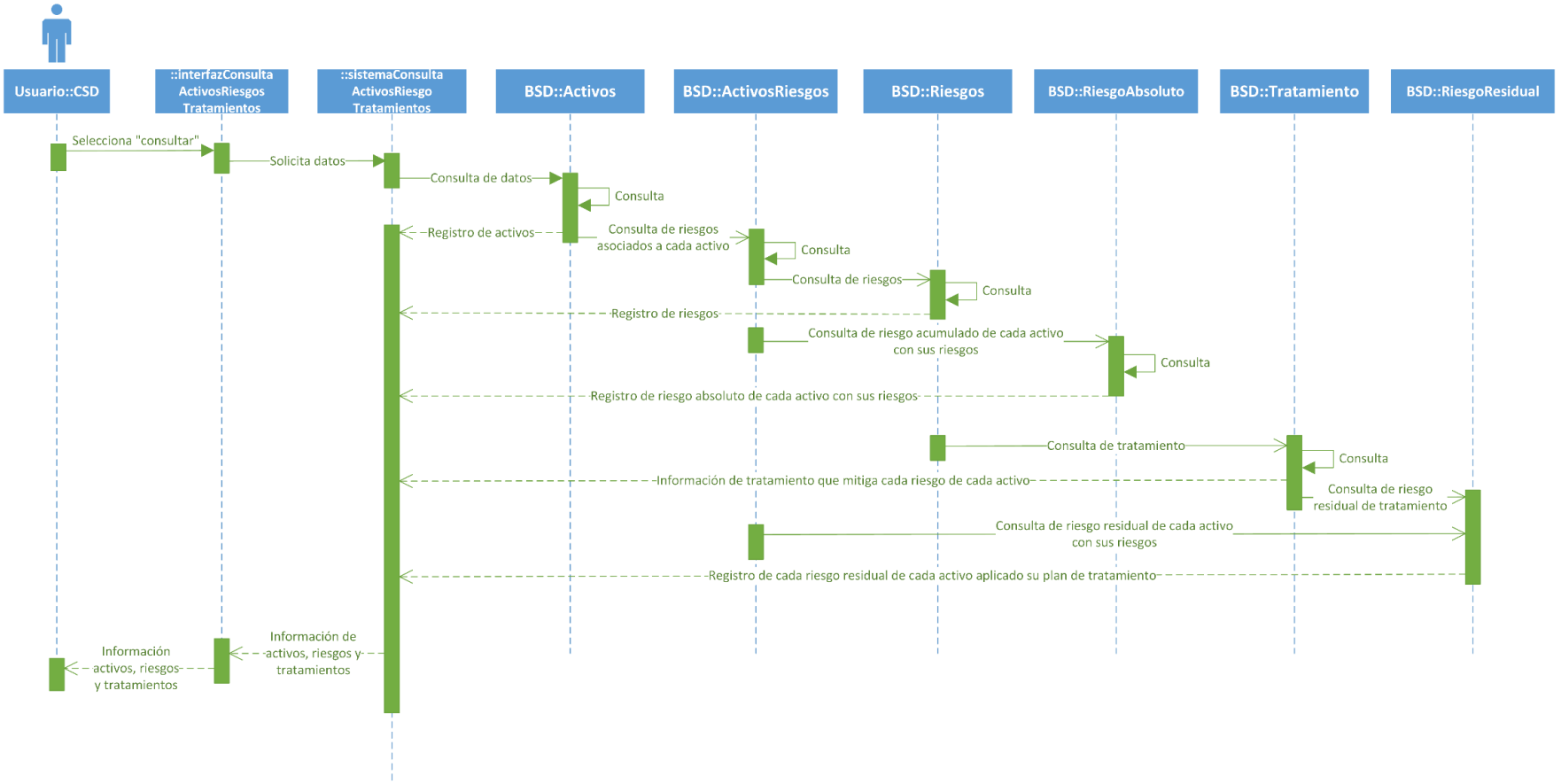

Ilustración 43: Relación entre activos, riesgos y planes de tratamiento.
Fuente: Elaboración propia.

Gestión de incidentes

La ilustración 44 representa el registro de incidentes suscitados en la empresa:

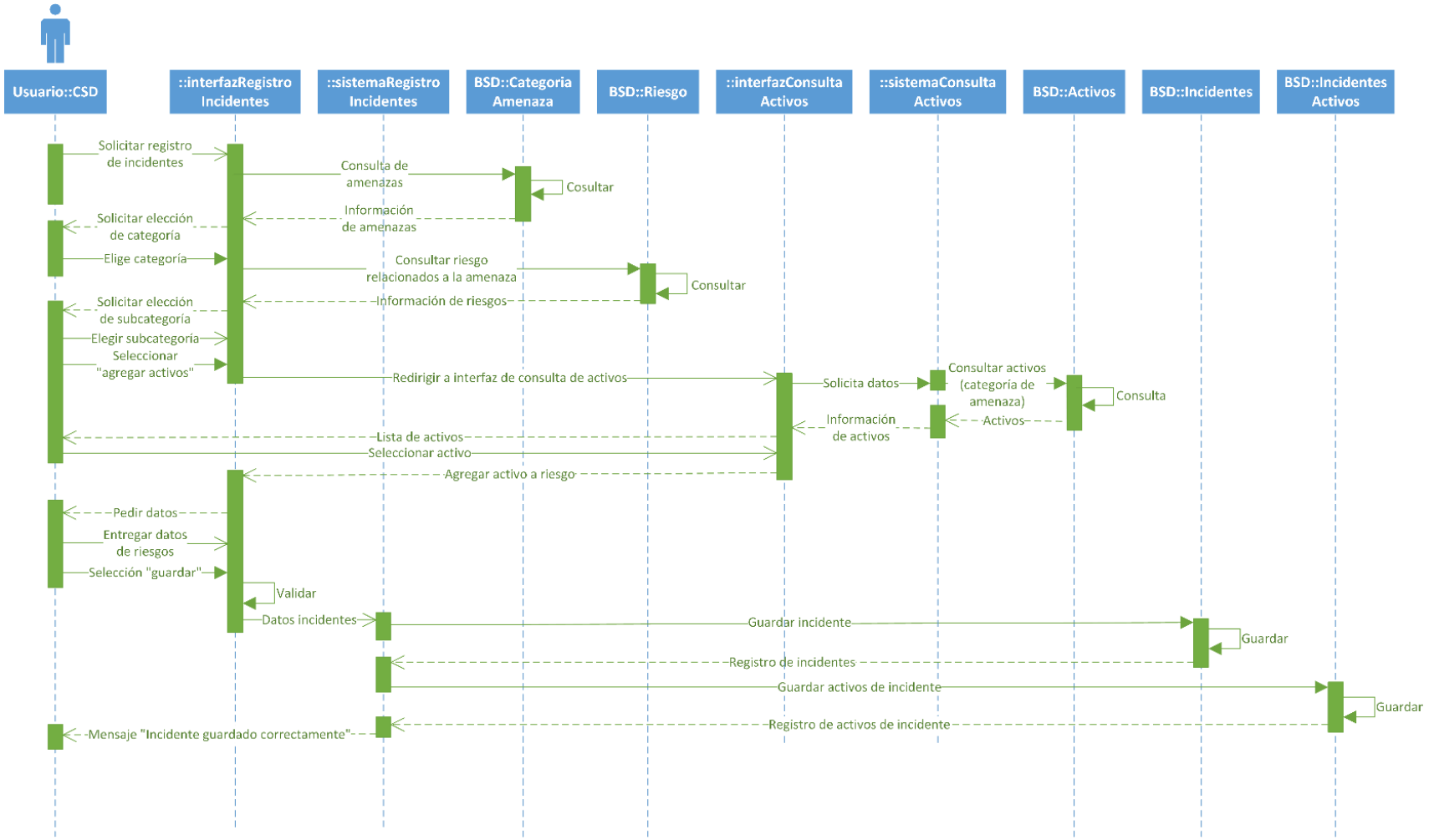

Ilustración 44: Registro de incidentes de la empresa.
Fuente: Elaboración propia.

La ilustración 45 representa la consulta de los incidentes que se hayan registrado en el sistema:

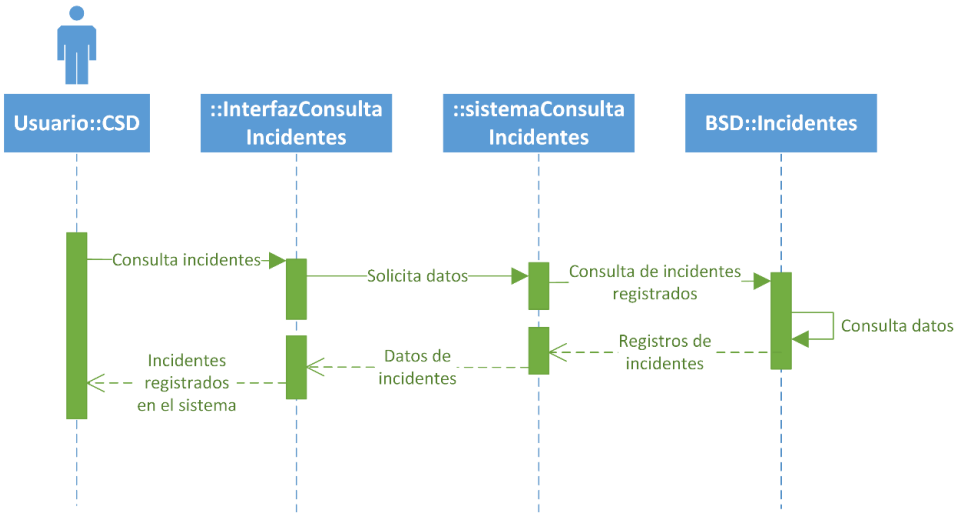

Ilustración 45:Consulta de incidentes registrados en el sistema.
Fuente: Elaboración propia.

La ilustración 46 representa la consulta de los detalles de un incidente que se haya registrado en el sistema:

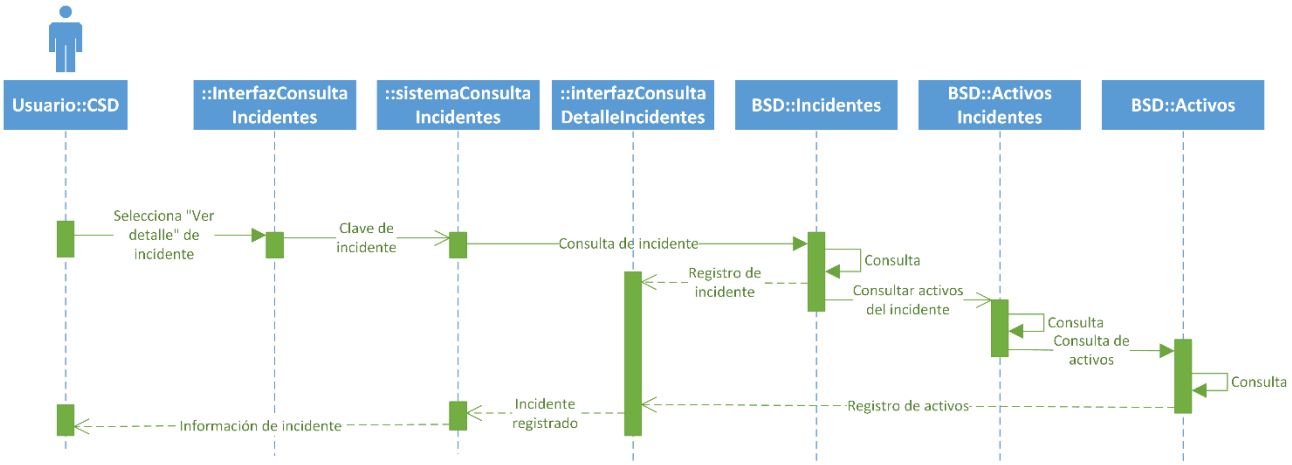

Ilustración 46: Consulta de detalles de un incidente registrado en el sistema.
Fuente: Elaboración propia.

La ilustración 47 representa la edición de un incidente que se haya registrado en el sistema:

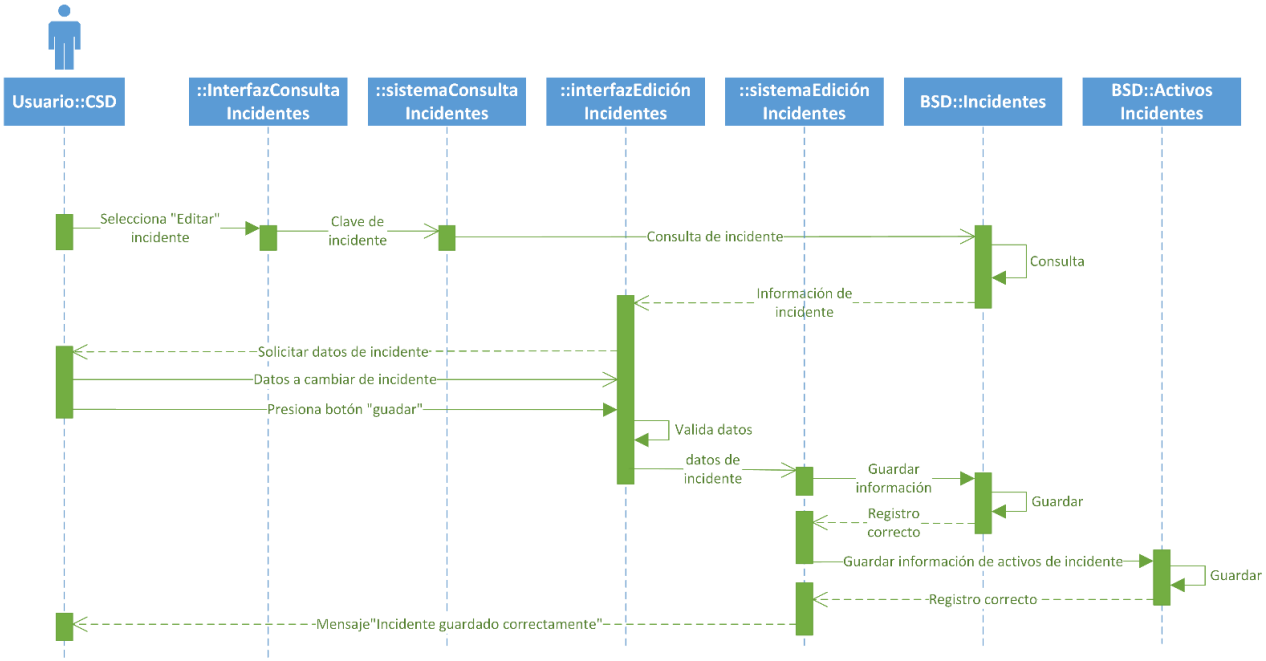

Ilustración 47: Edición de incidentes registrados en el sistema.
Fuente: Elaboración propia.

Gestión de procesos de negocio

La ilustración 48 representa el registro de un proceso de negocio en el sistema:

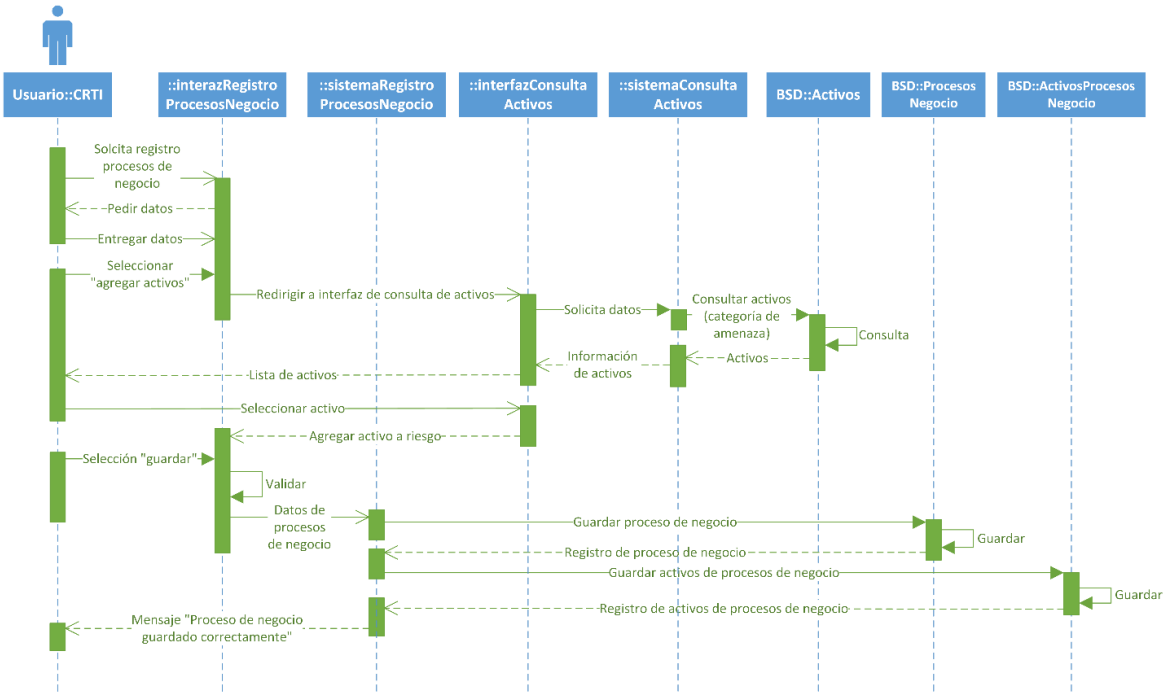

Ilustración 48: Registro de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 49 representa la consulta de los procesos de negocio registrados en el sistema:

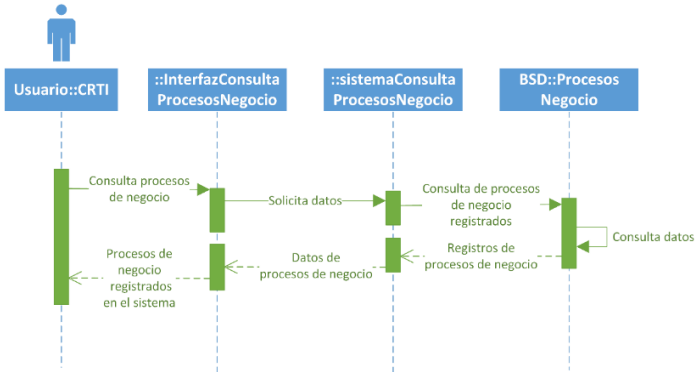

Ilustración 49: Consulta de procesos de negocio registrados en el sistema.
Fuente: Elaboración propia.

La ilustración 50 representa la consulta de los detalles de un proceso de negocio registrado en el sistema:

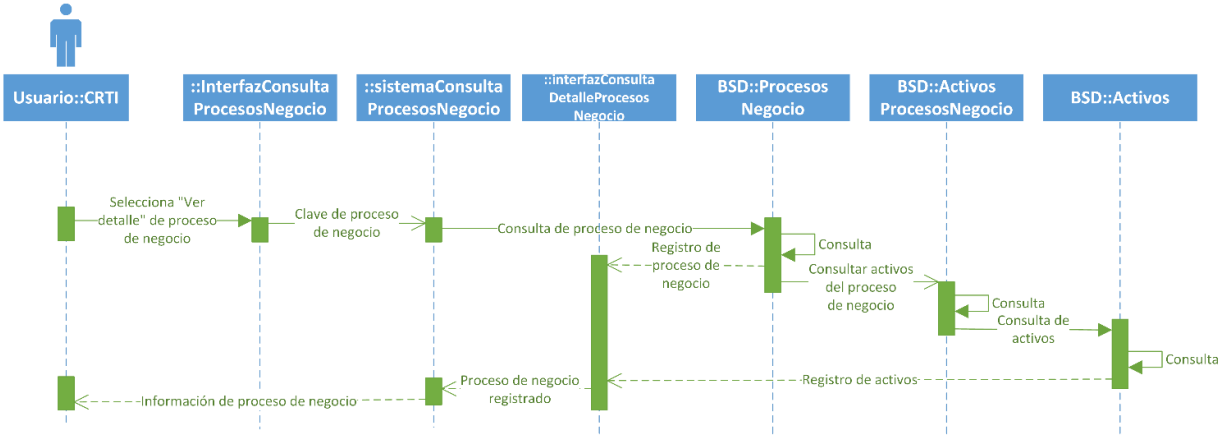

Ilustración 50: Ilustración 50: Consulta de detalles de un proceso de negocio registrado en el sistema.
Fuente: Elaboración propia.

La ilustración 51 representa la edición de información de un proceso de negocio registrado en el sistema:

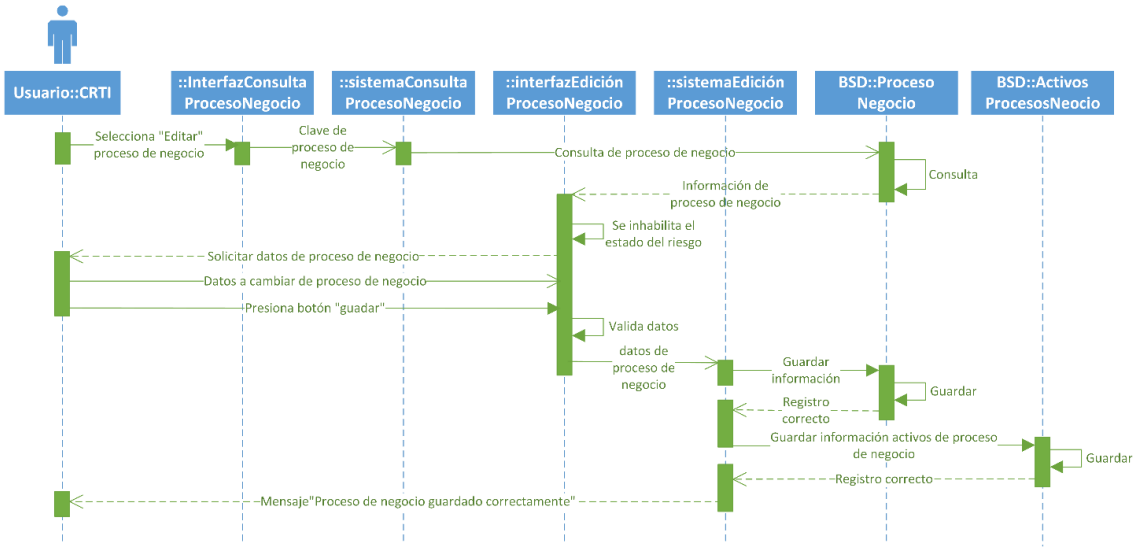

Ilustración 51: Edición de información de un proceso de negocio.
Fuente: Elaboración propia.

La ilustración 52 representa el registro de baja o registro de alta de un proceso de negocio de la organización:

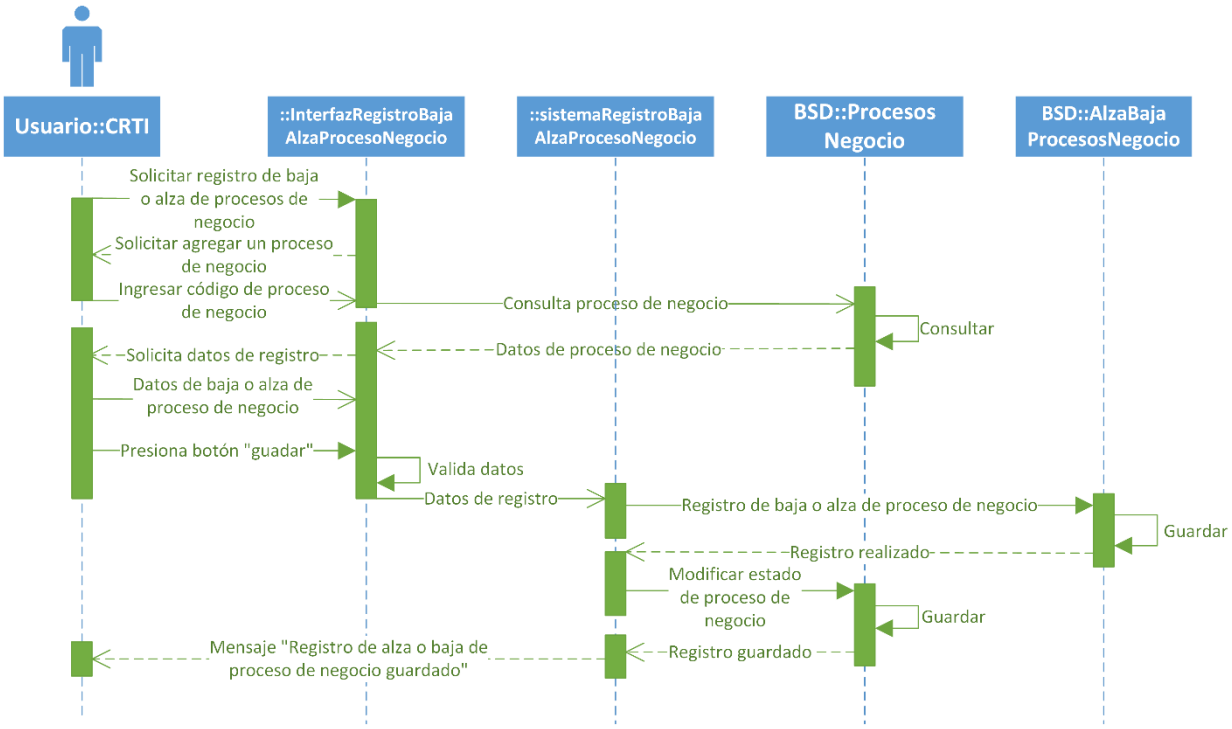

Ilustración 52: Registro de baja o alta de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 53 representa la consulta de los registros de baja o registro de alta de los procesos de negocio de la organización registrados en el sistema:

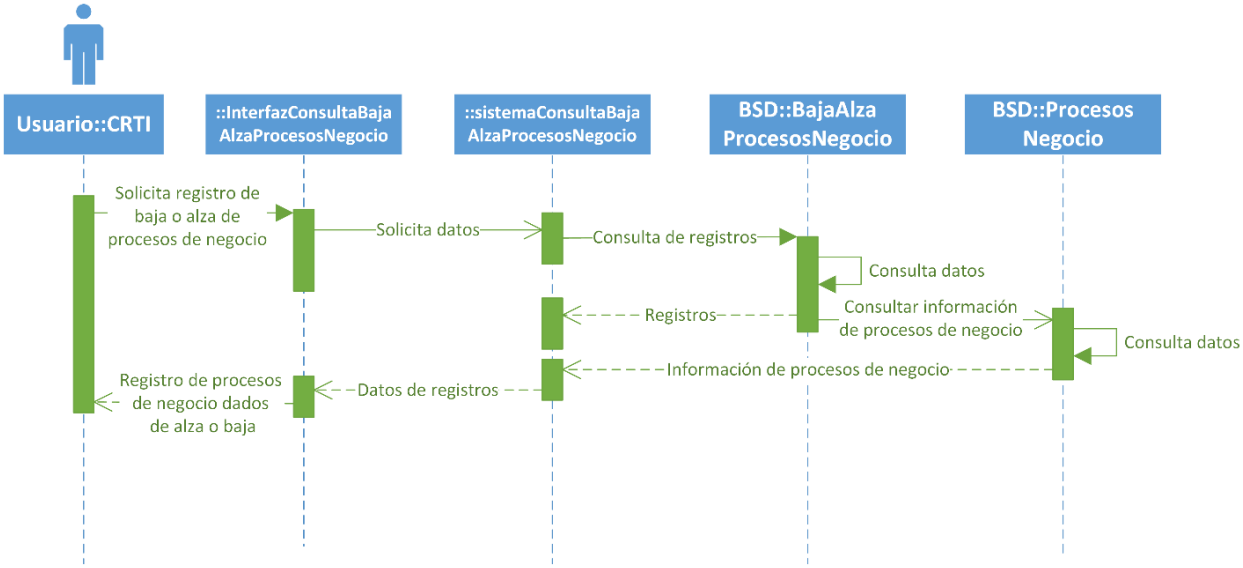

Ilustración 53: Consulta de procesos de negocio dados de baja o alta.
Fuente: Elaboración propia.

La ilustración 54 representa el registro de incidentes que se pudieran suscitar dentro de los procesos de negocio, entonces entran al sistema como un proceso de negocio en seguimiento:

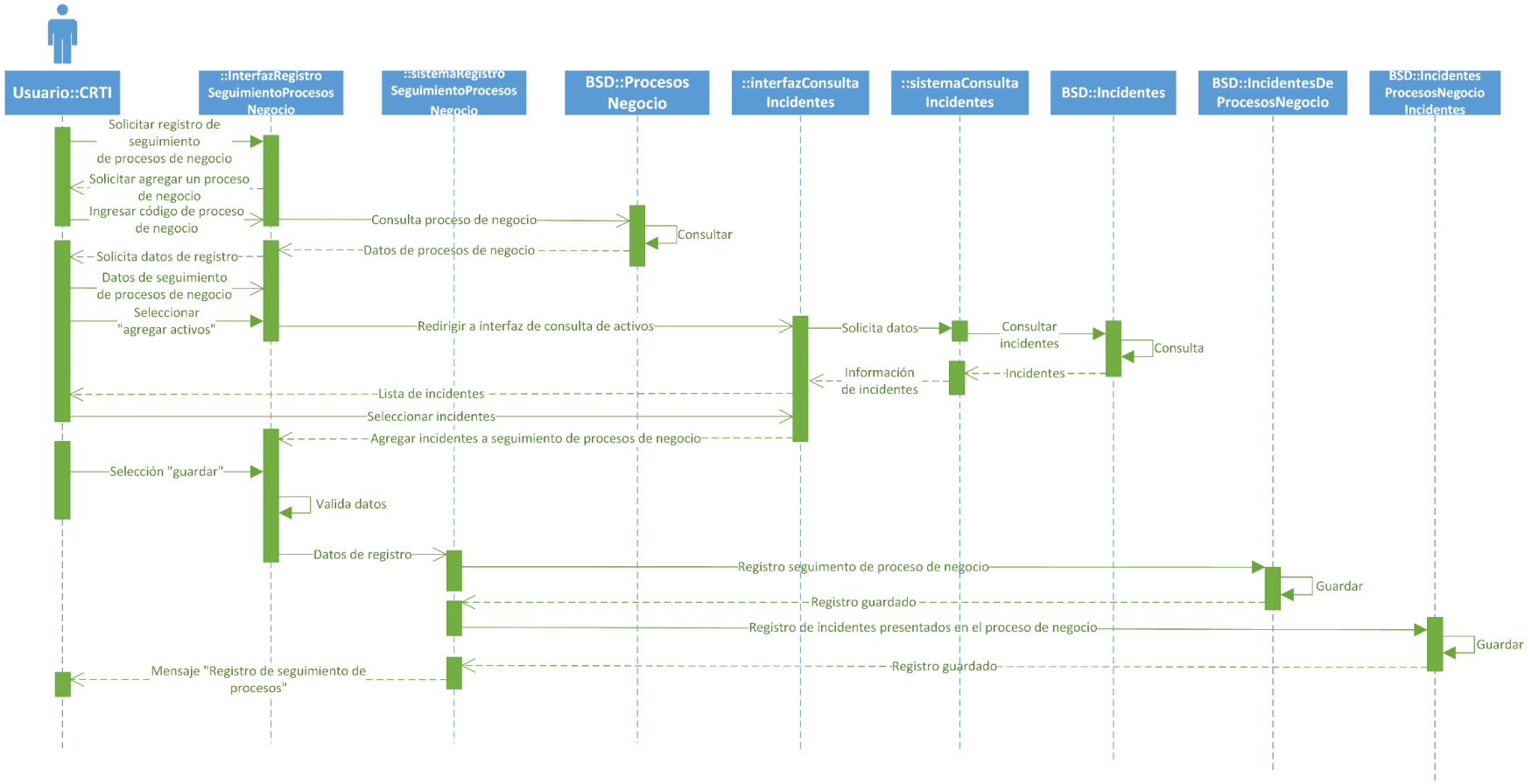

Ilustración 54: Registro de seguimiento de procesos de negocio.
Fuente: Elaboración propia.

La ilustración 55 representa la consulta de los procesos de negocio que estén en seguimiento, es decir, en los cuales se hayan suscitado incidentes.

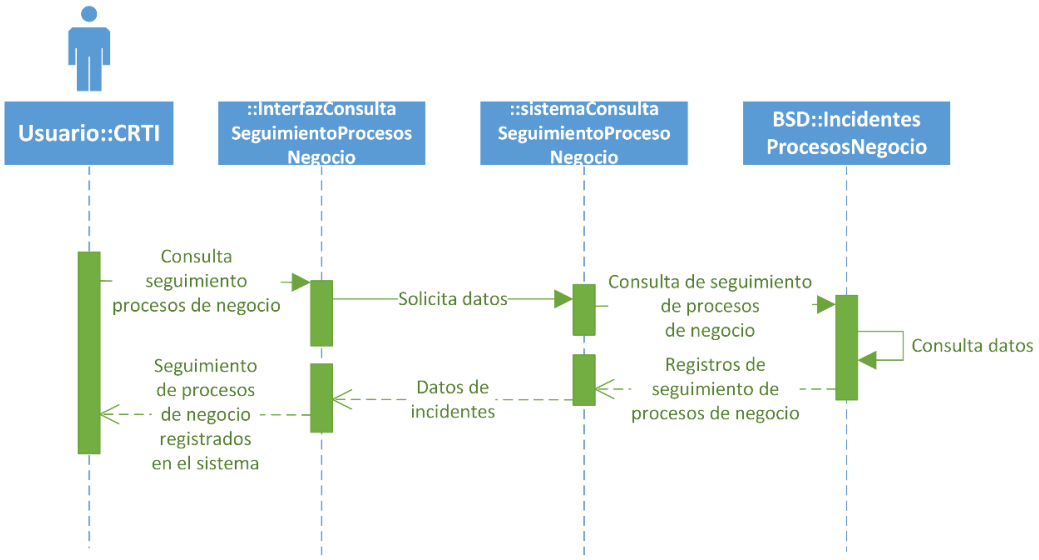

Ilustración 55: Consulta de procesos de negocio en seguimiento.
Fuente: Elaboración propia.

La ilustración 56 representa la consulta del detalle de un proceso de negocio registrado en seguimiento:

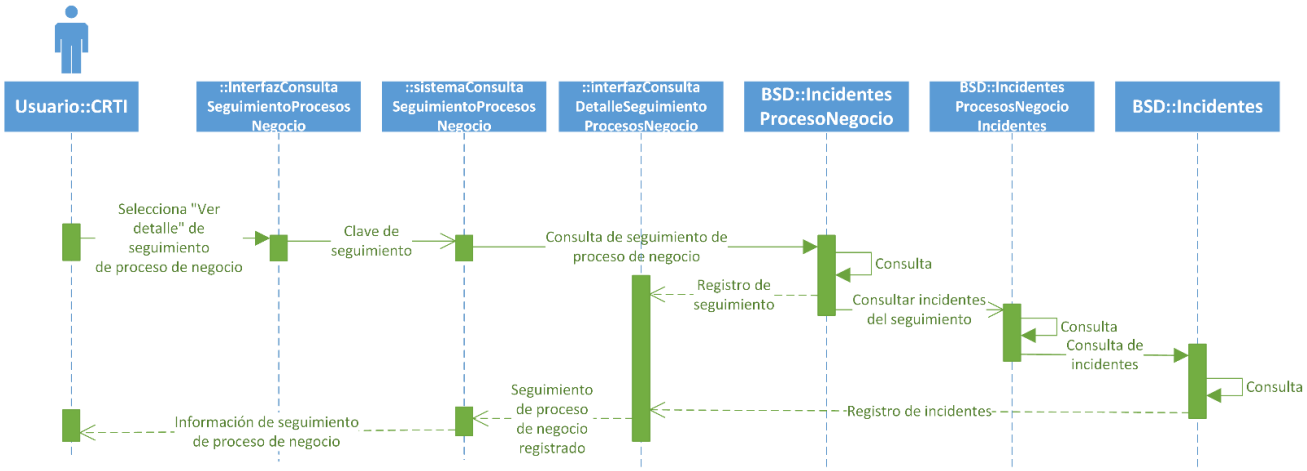

Ilustración 56: Consulta de detalles de un proceso de negocio registrado en seguimiento.
Fuente: Elaboración propia.

La ilustración 57 representa la edición de información del seguimiento de proceso de negocio registrado en el sistema:

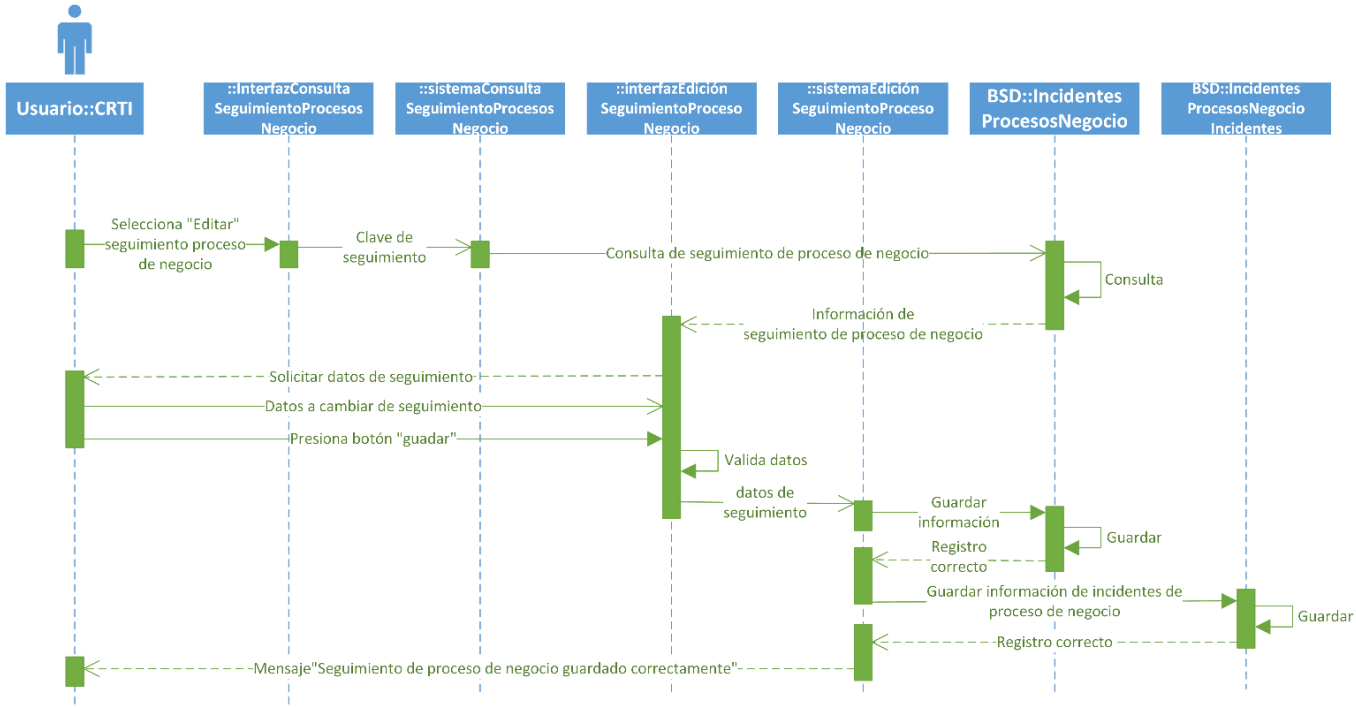

Ilustración 57: Edición de información de seguimiento de procesos de negocio.
Fuente: Elaboración propia.

Reportes

La ilustración 58 representa un reporte de cuadro de mando integrado (CMI), en donde, se relaciona cada proceso de negocio y todos sus activos que lo componen; con cada activo se muestran los riesgos que tiene cada uno, también el tratamiento registrado que lo mitiga (si lo tiene), como información adicional se muestra n los riesgos absolutos y residuales de cada uno:

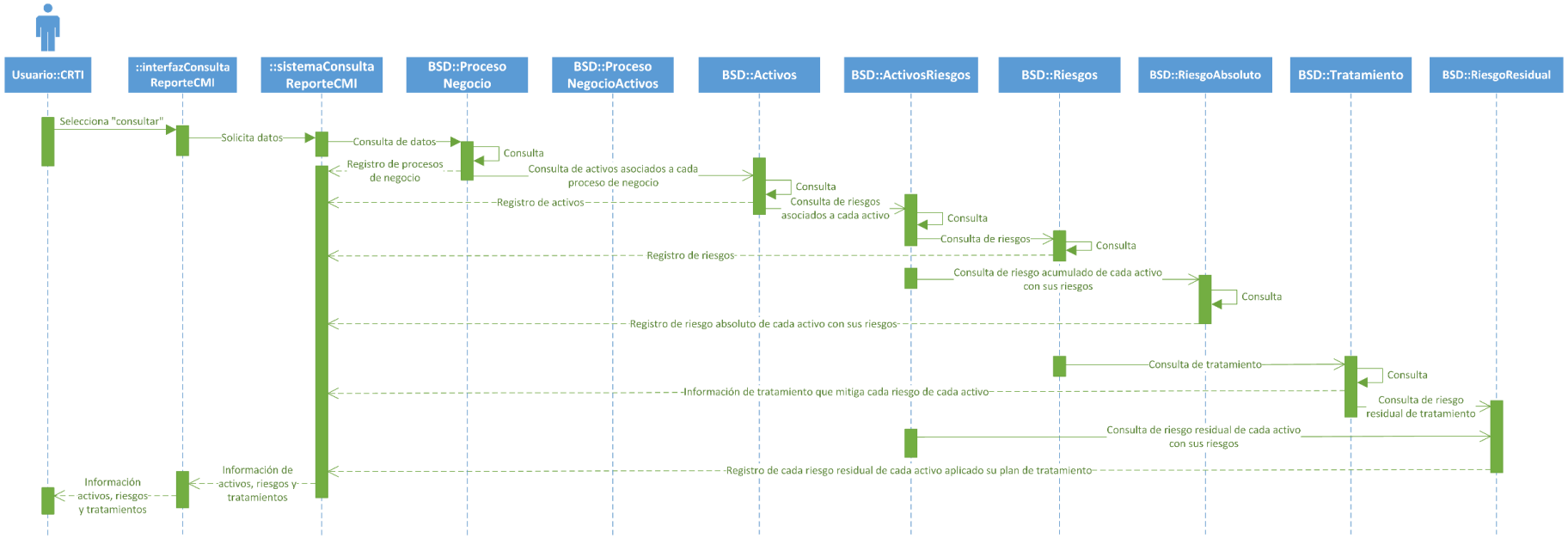

Ilustración 58: Cuadro de mando integrado.
Fuente: Elaboración propia.

La ilustración 59 representa el reporte de indicadores clave de desempeño de incidentes registrados:

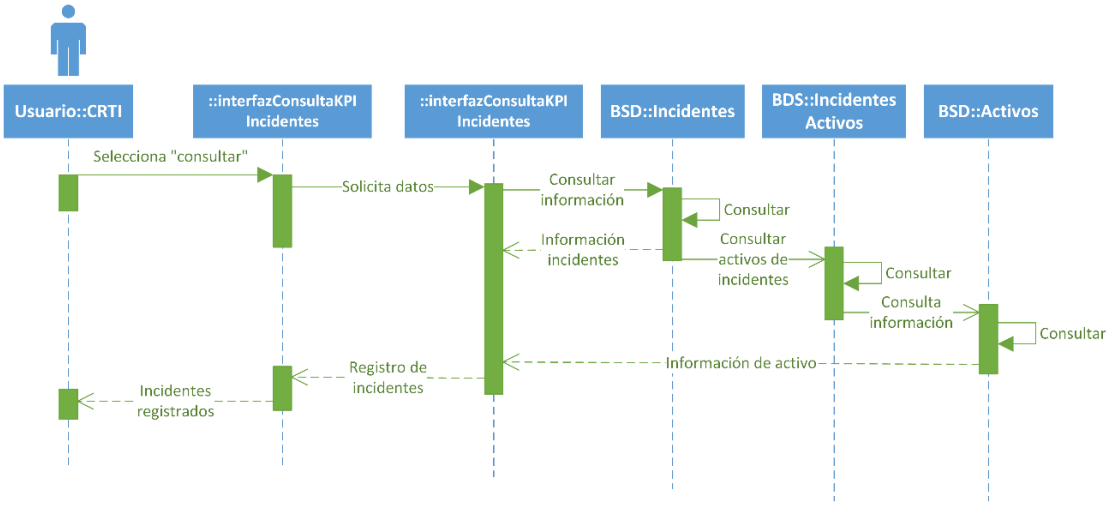

Ilustración 59:Reporte de indicadores clave de desempeño de incidentes.
Fuente: Elaboración propia.

La ilustración 60 representa el reporte de indicadores clave de desempeño de procesos de negocio:

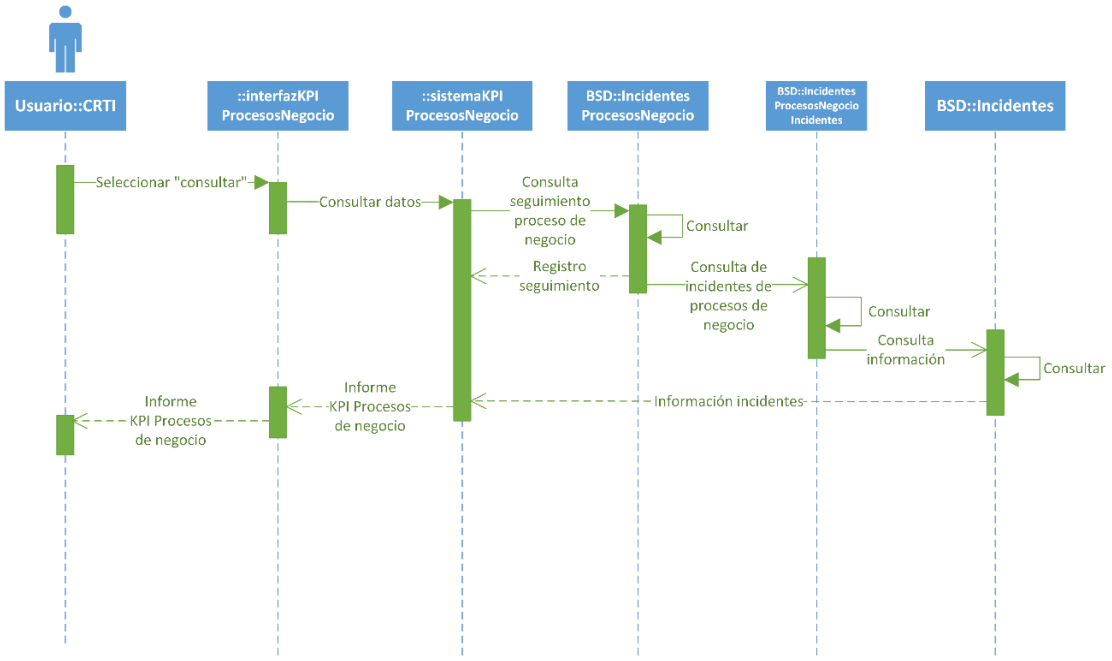

Ilustración 60: Reporte de indicadores clave de desempeño de procesos de negocio.
Fuente: Elaboración propia.

La siguiente ilustración 61 representa el reporte de indicadores clave de desempeño de planes de tratamiento registrados:

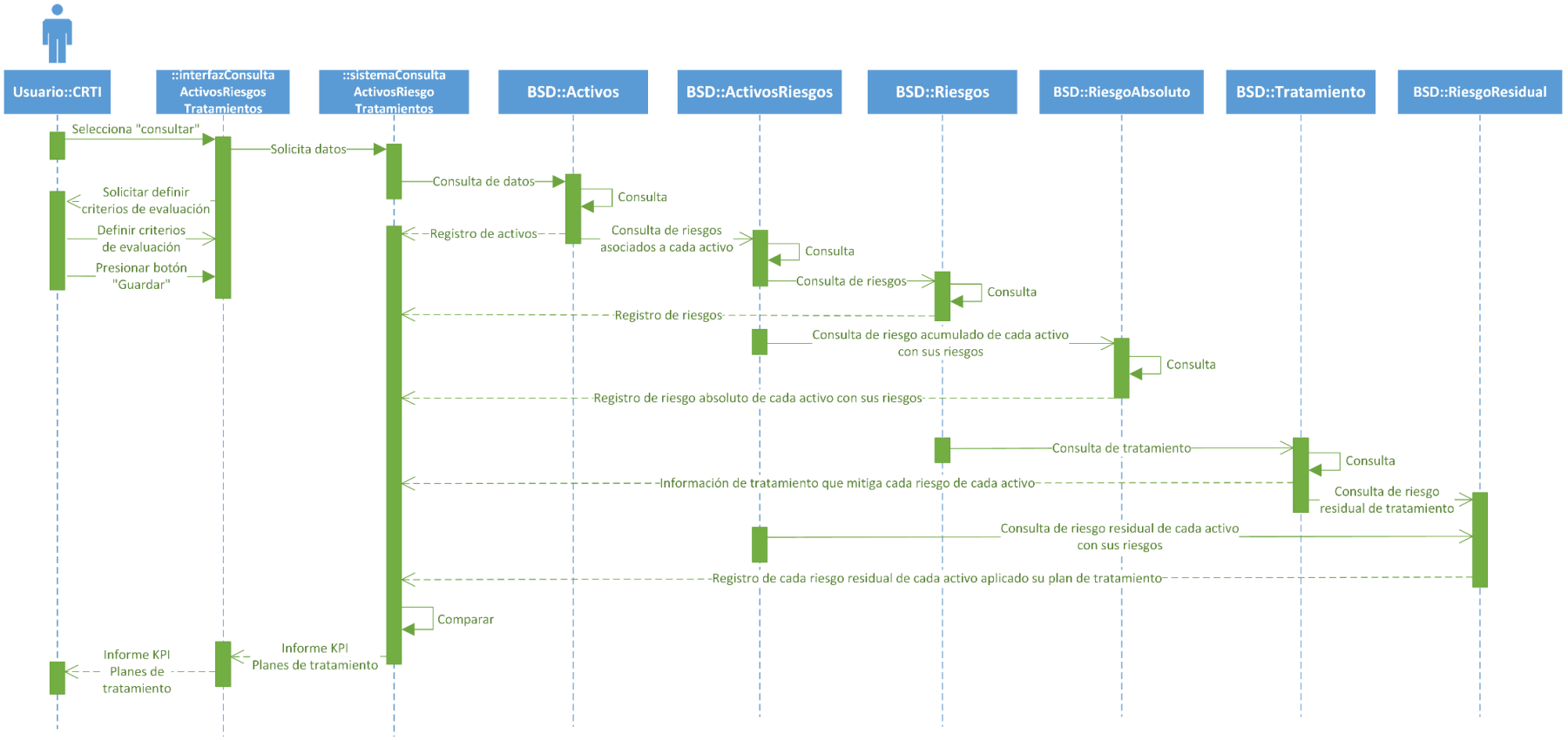

Ilustración 61: Reporte de indicadores clave de desempeño de planes de tratamiento.
Fuente: Elaboración propia.

Gestión de usuarios

La ilustración 62 representa el registro de un usuario:

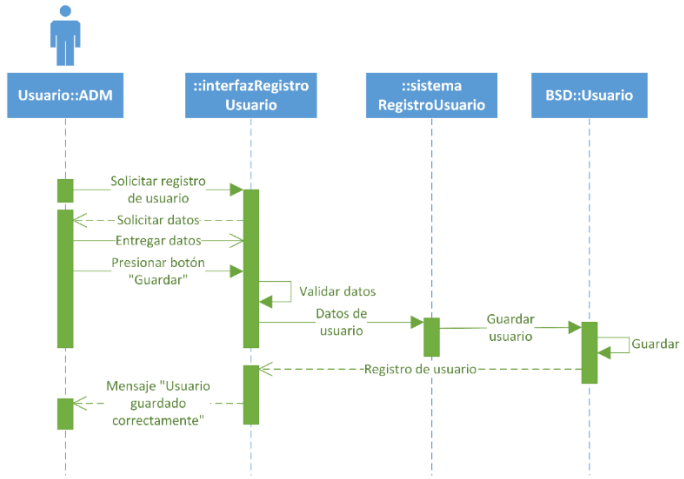

Ilustración 62: Registro de usuario.
Fuente: Elaboración propia.

La ilustración 63 representa la consulta de usuarios registrados en el sistema:

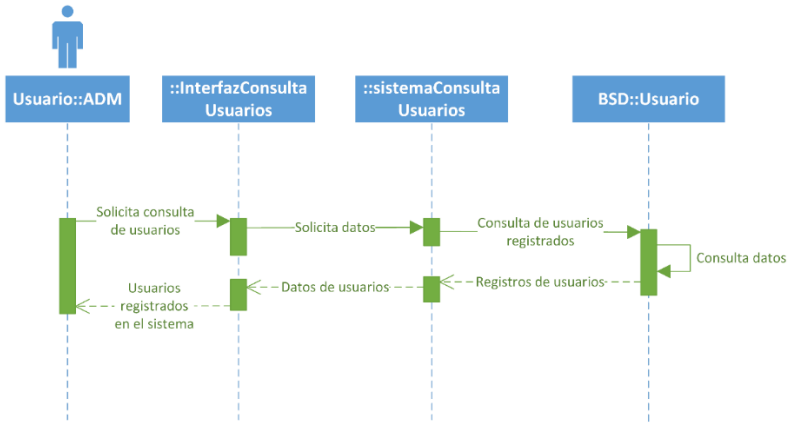

Ilustración 63: Consulta de usuarios registrados en el sistema.
Fuente: Elaboración propia.

La ilustración 64 representa la consulta de detalles de un usuario registrado en el sistema:

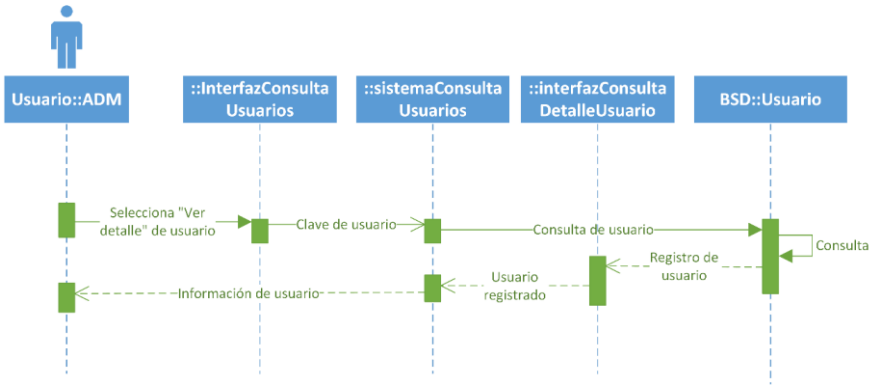

Ilustración 64: Consulta de detalles de un usuario.
Fuente: Elaboración propia.

La ilustración 65 representa la edición de información de un usuario registrado en el sistema:

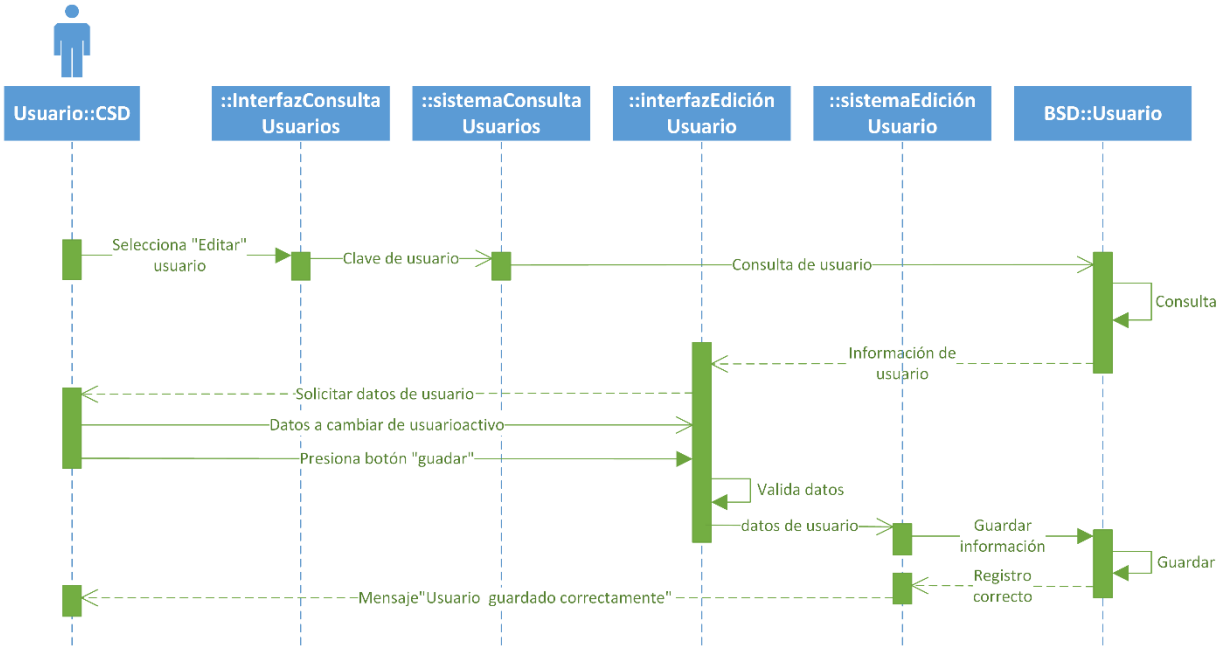

Ilustración 65: Edición de información de usuario.
Fuente: Elaboración propia.

4.4. Modelo funcional

García Chi (2013) manifiesta que dentro del modelo funcional son abordados dos elementos:

- La funcionalidad observable respecto al usuario.
- Las operaciones que se suscitan dentro de las clases de análisis, que representan comportamientos.

Este modelo es representado mediante el diagrama de actividades, que es un esquema que muestra la descomposición de una actividad en sus componentes. (Rumbaugh, Jacobson, & Booch, 2004)

4.4.1. Diagramas de actividades del software Ecu@Risk

Inicio de sesión

La ilustración 66 representa el inicio de sesión de un usuario:

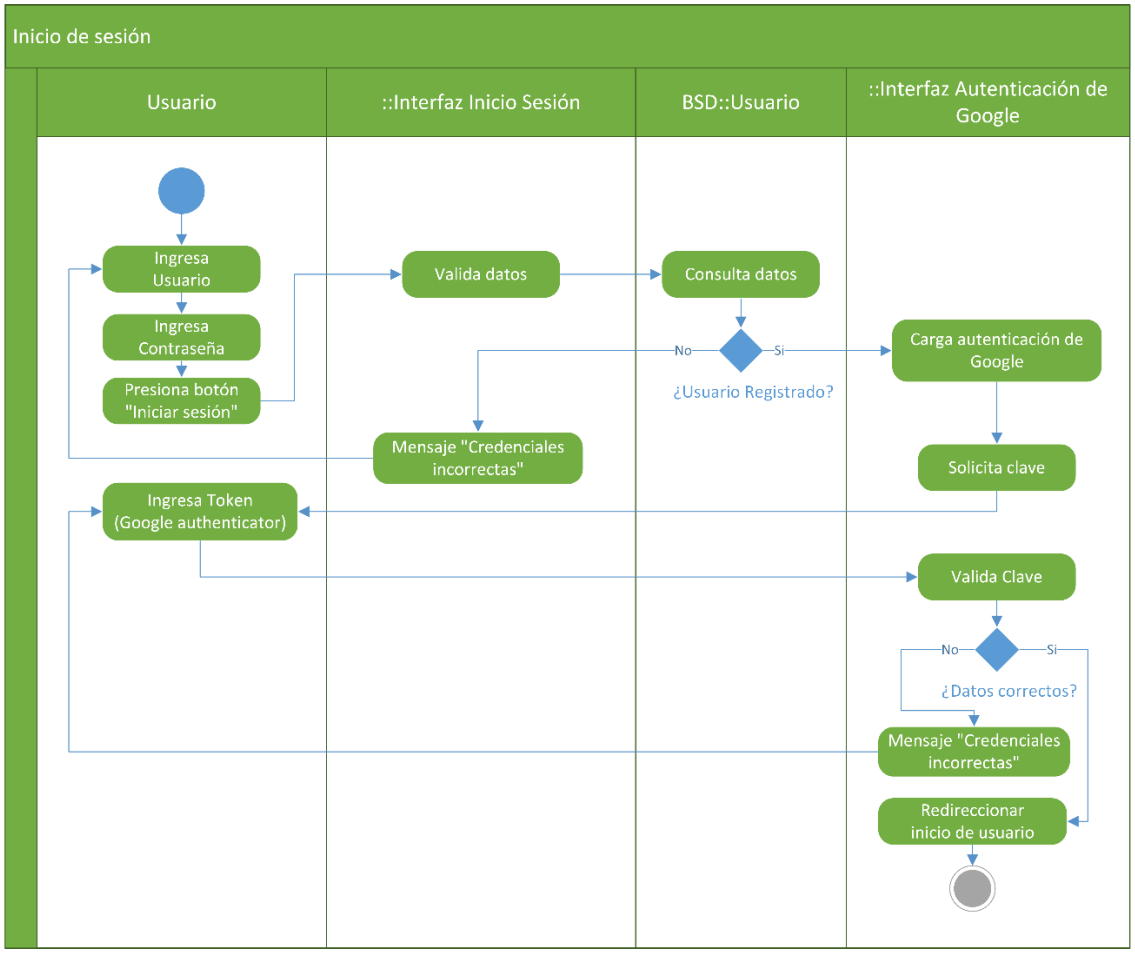

Ilustración 66: Inicio de sesión de usuario.
Fuente: Elaboración propia.

Gestión de activos de información

La ilustración 67 representa el registro de un activo de edificación:

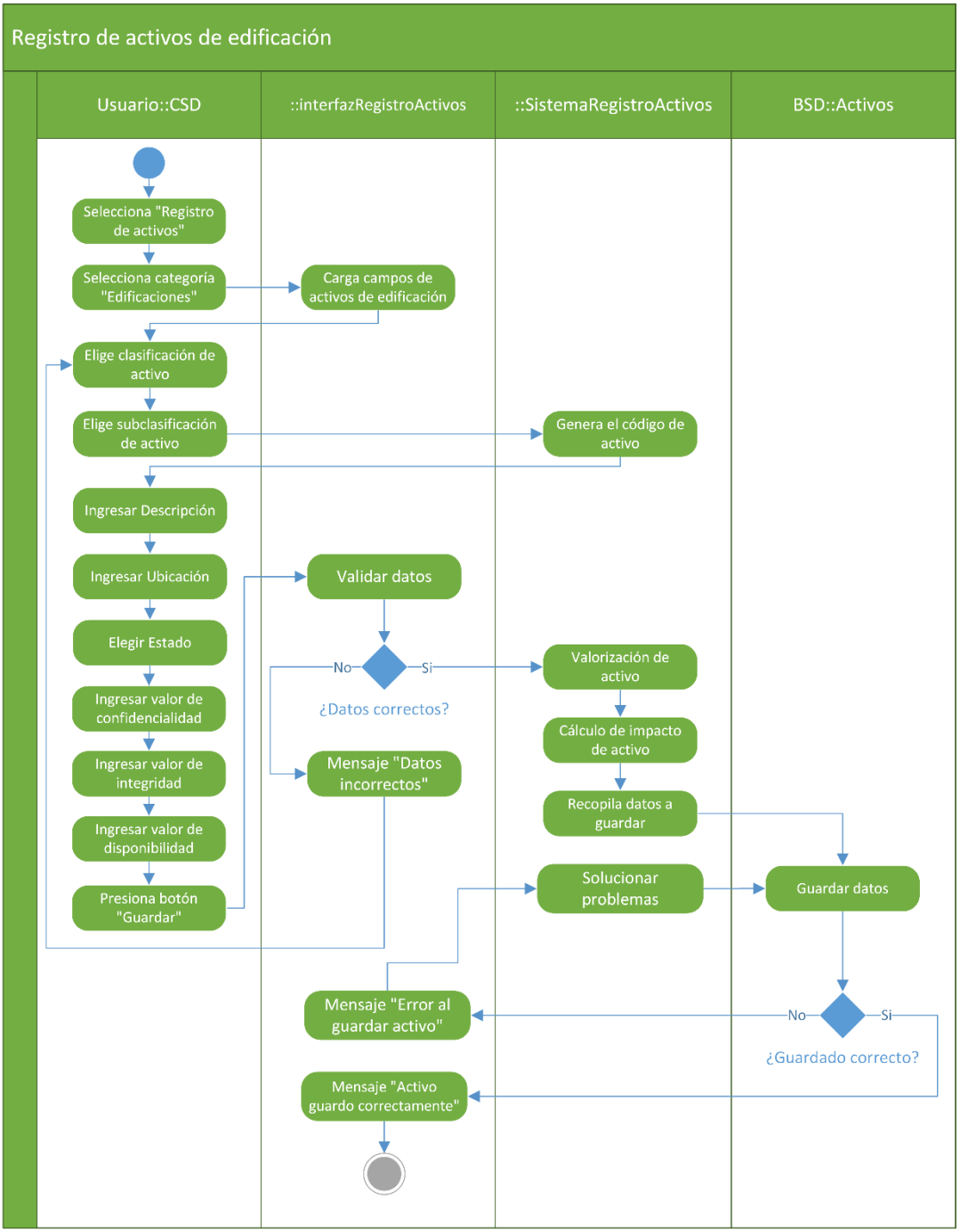

Ilustración 67: Registro de activos de información de edificación.
Fuente: Elaboración propia.

La ilustración 68 representa el registro de activos de información de hardware:

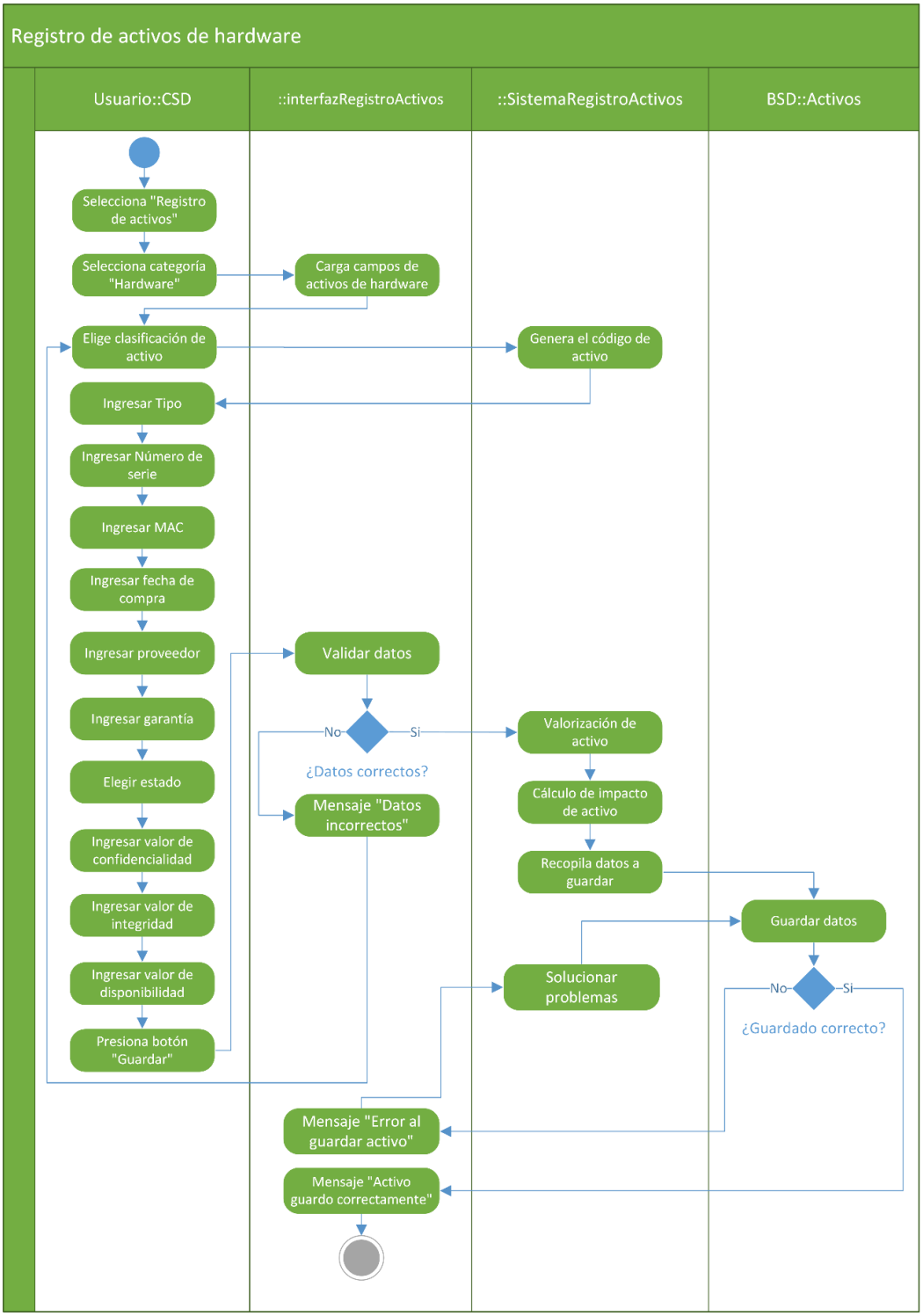

Ilustración 68: Registro de activos de información de hardware.
Fuente: Elaboración propia.

La ilustración 69 representa el registro de activos de información de software:

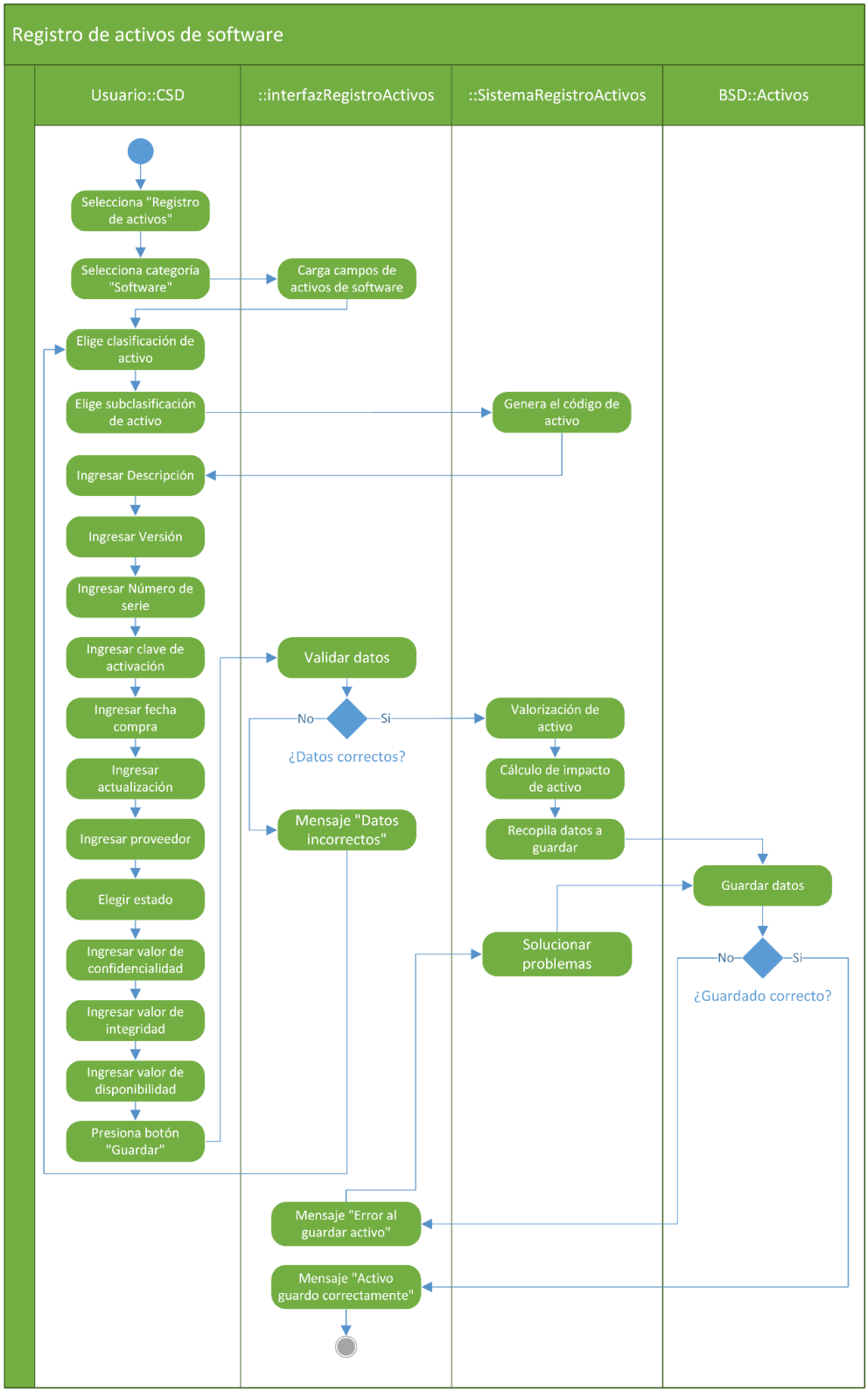

Ilustración 69: Registro de activos de información de software.
Fuente: Elaboración propia.

La ilustración 70 representa el registro de activos de información electrónica: La ilustración 70 representa el registro de activos de información electrónica:

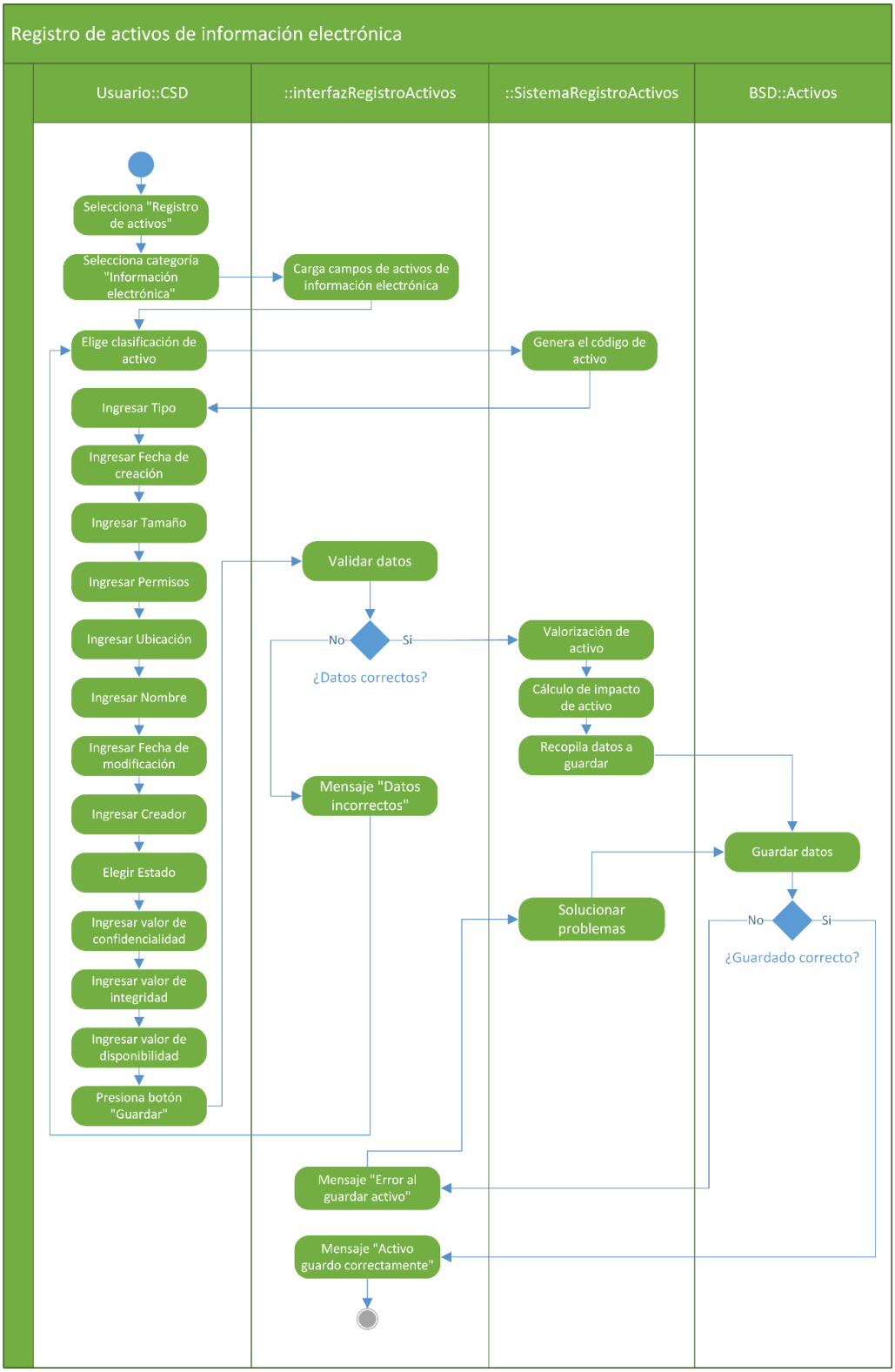

Ilustración 70: Registro de activos de información electrónica.
Fuente: Elaboración propia.

La ilustración 71 representa el registro de activos de información en papel:

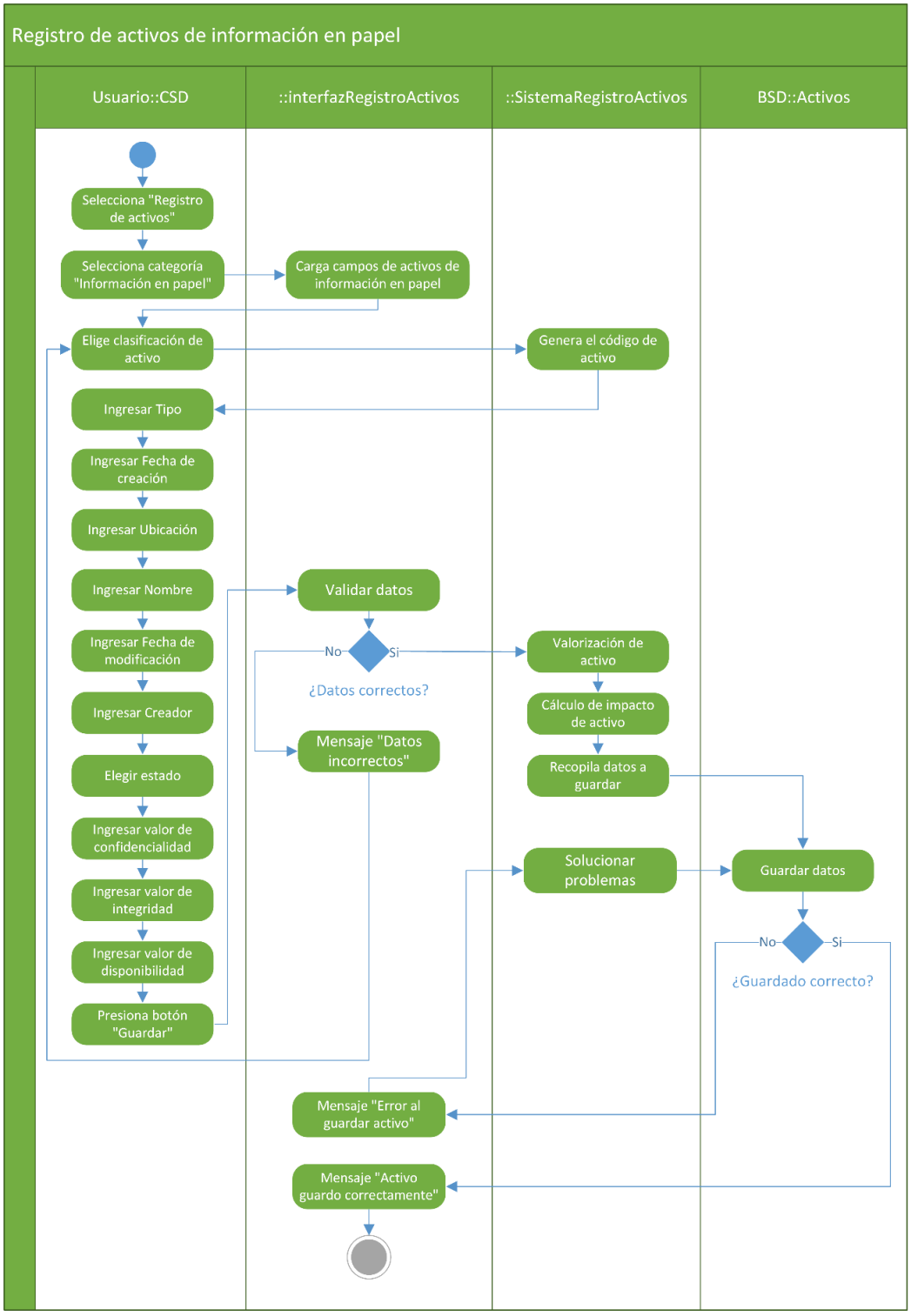

Ilustración 71: Registro de activos de información en papel.
Fuente: Elaboración propia.

La ilustración 72 representa el registro de activos de información de infraestructura de comunicaciones:

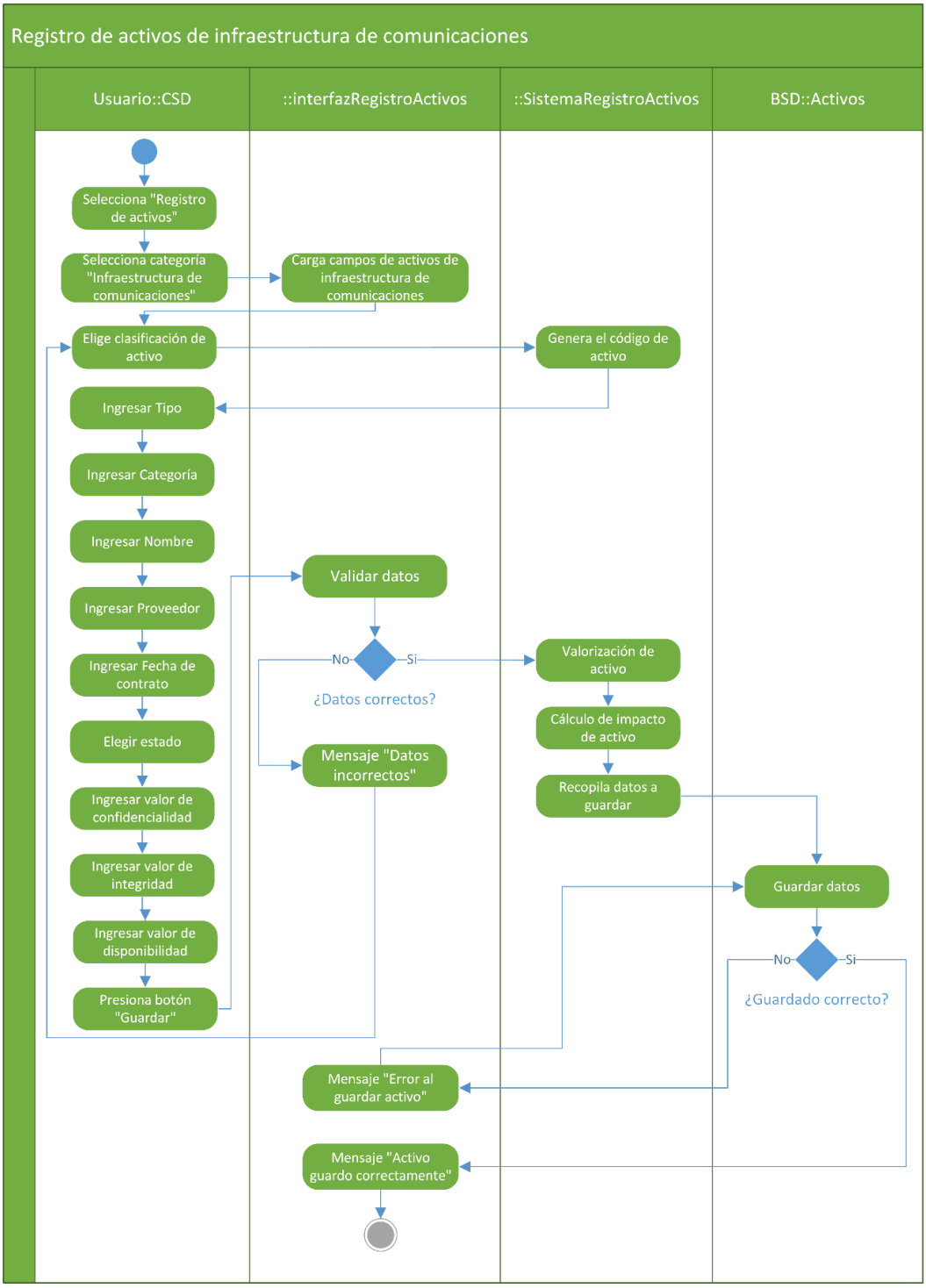

Ilustración 72: Registro de activos de infraestructura de comunicaciones.
Fuente: Elaboración propia

La ilustración 73 representa el registro de activos de información de medios de almacenamiento extraíble:

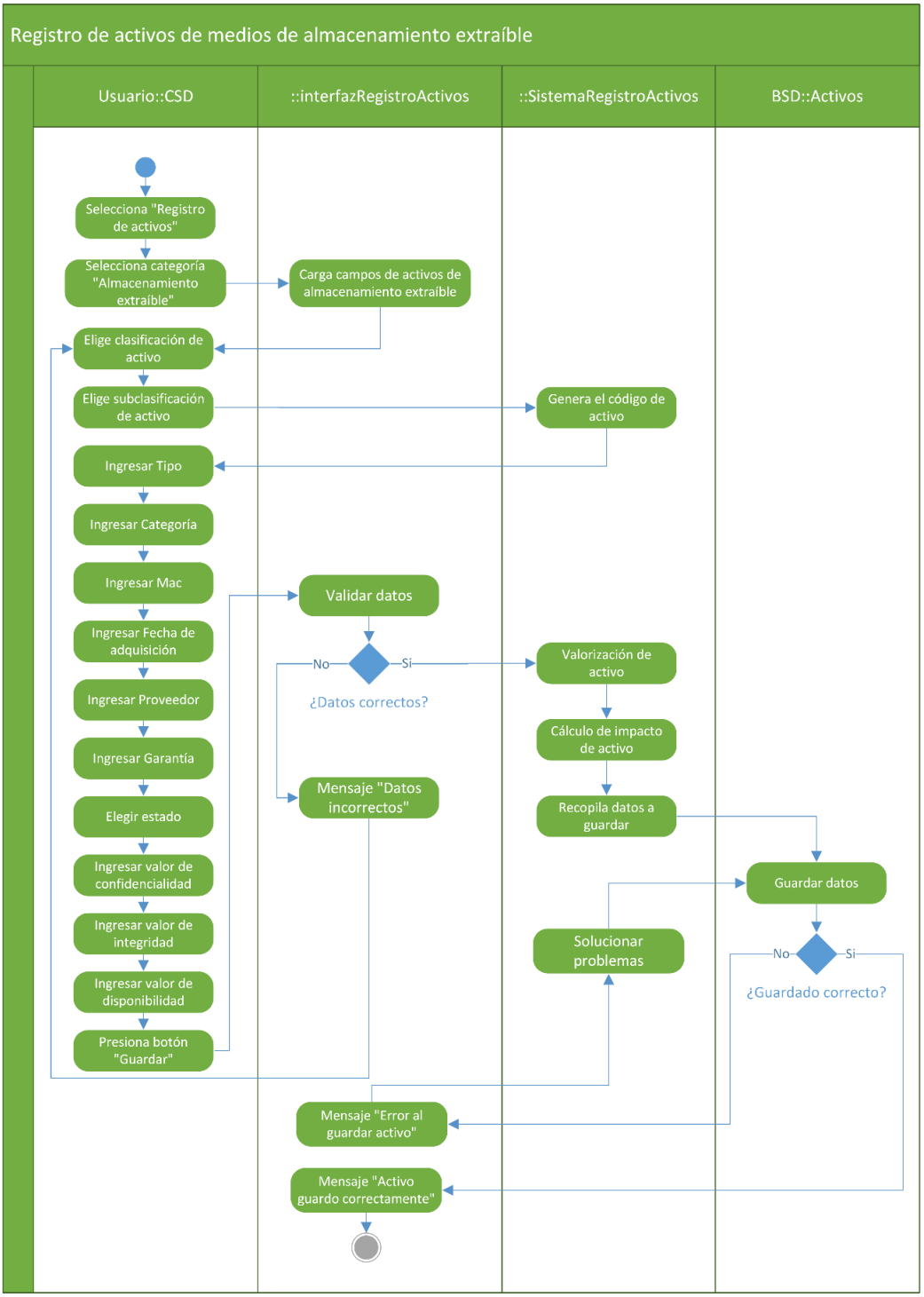

Ilustración 73: Registro de activos de información de medios de almacenamiento extraíble.
Fuente: Elaboración propia.

La ilustración 74 representa el registro de activos de información recursos humanos:

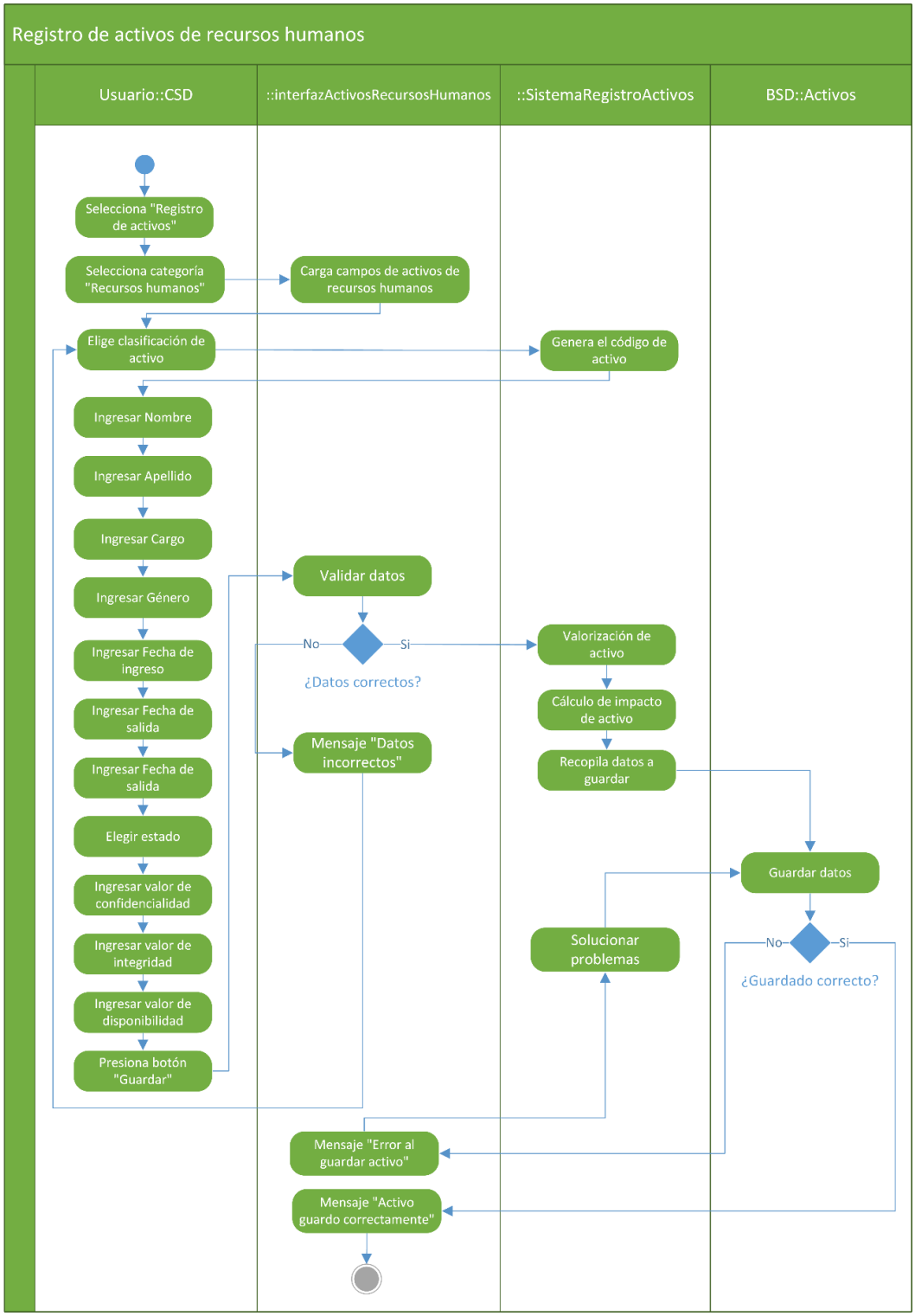

Ilustración 74: Registro de activos de información de recursos humanos.
Fuente: Elaboración propia.

La ilustración 75 representa la consulta de los activos de información registrados en el sistema:

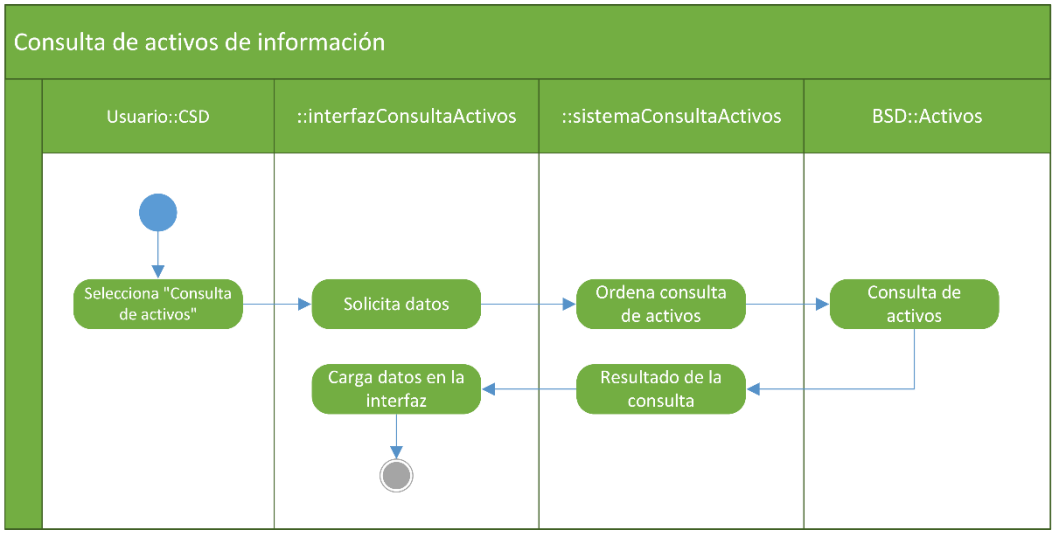

Ilustración 75: Consulta de activos de información.
Fuente: Elaboración propia.

La ilustración 76 representa la consulta de los detalles de un activo de información registrado en el sistema:

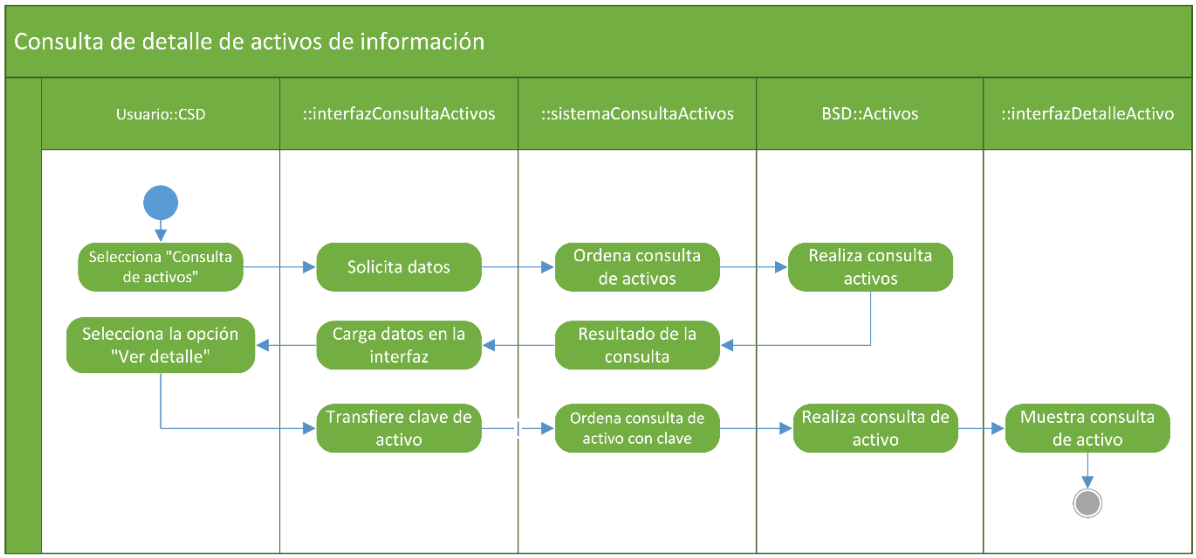

Ilustración 76: Consulta de detalles de un activo de información.
Fuente: Elaboración propia.

La ilustración 77 representa la edición de información de un activo de información:

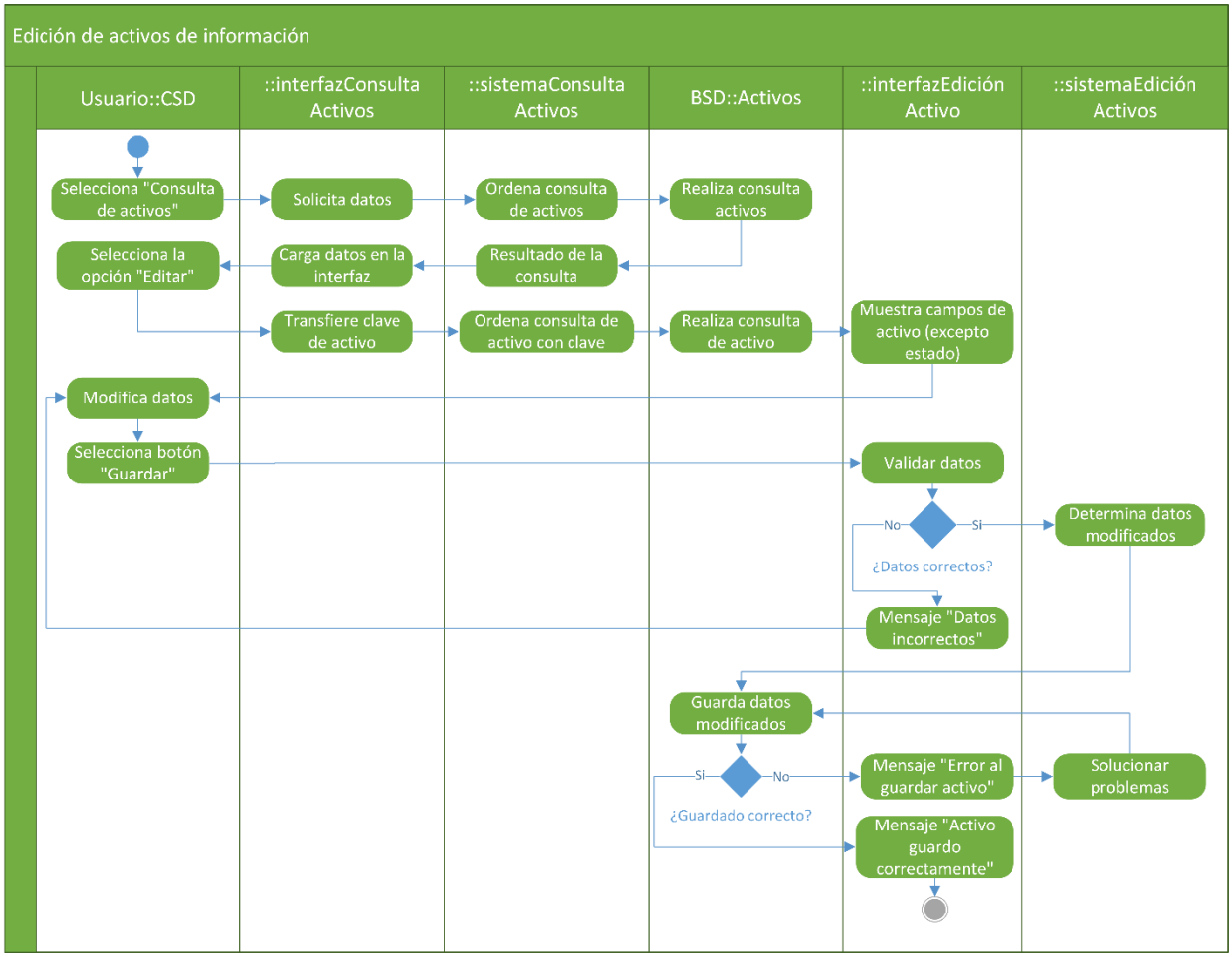

Ilustración 77:Edición de información de activo de información. Fuente: Elaboración propia

La ilustración 78 representa el registro de baja o registro de alta de activos de información:

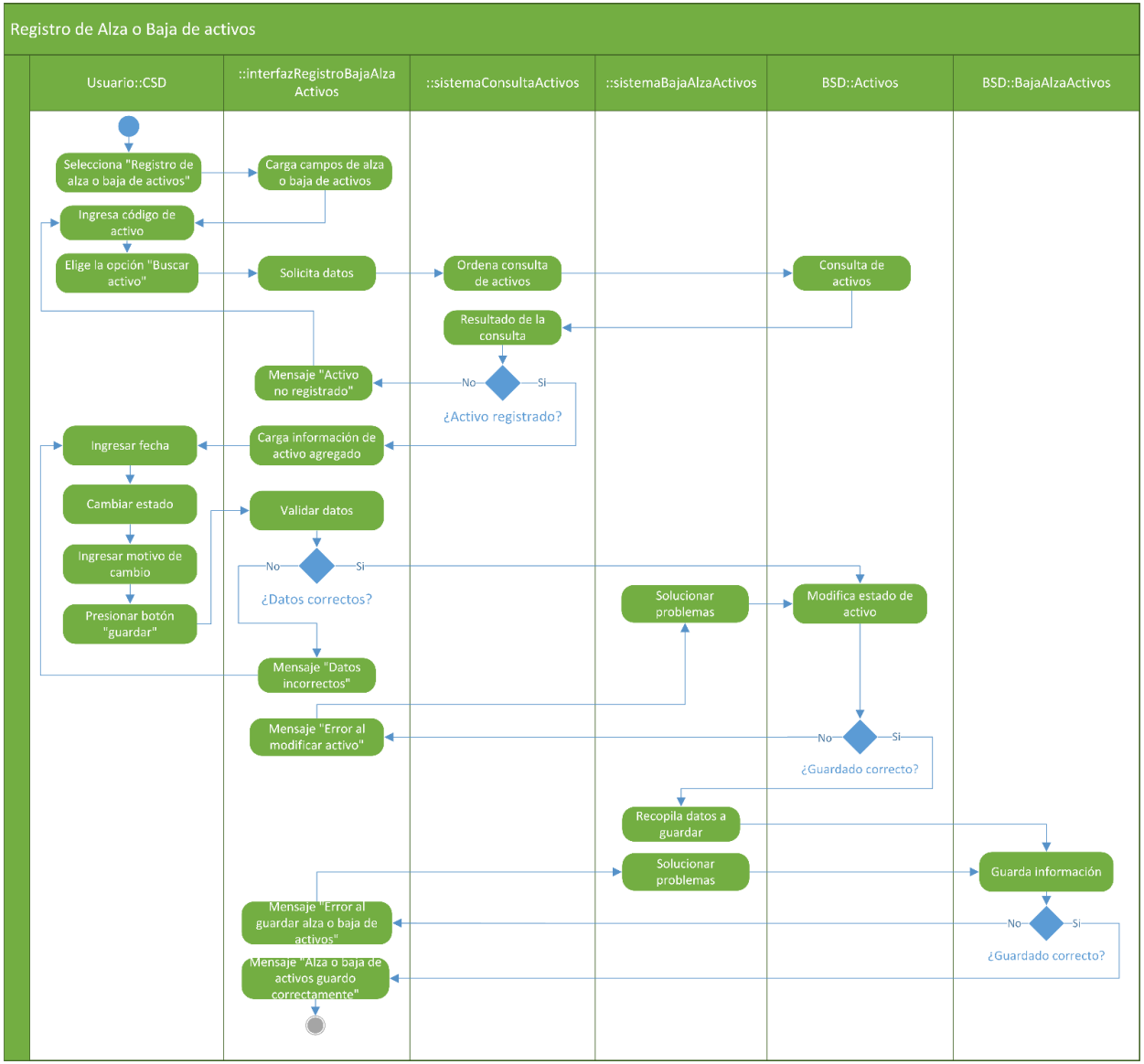

Ilustración 78: Registro alta o baja de activo de información.
Fuente: Elaboración propia.

La ilustración 79 representa el registro de baja o registro de alta de activos de información:

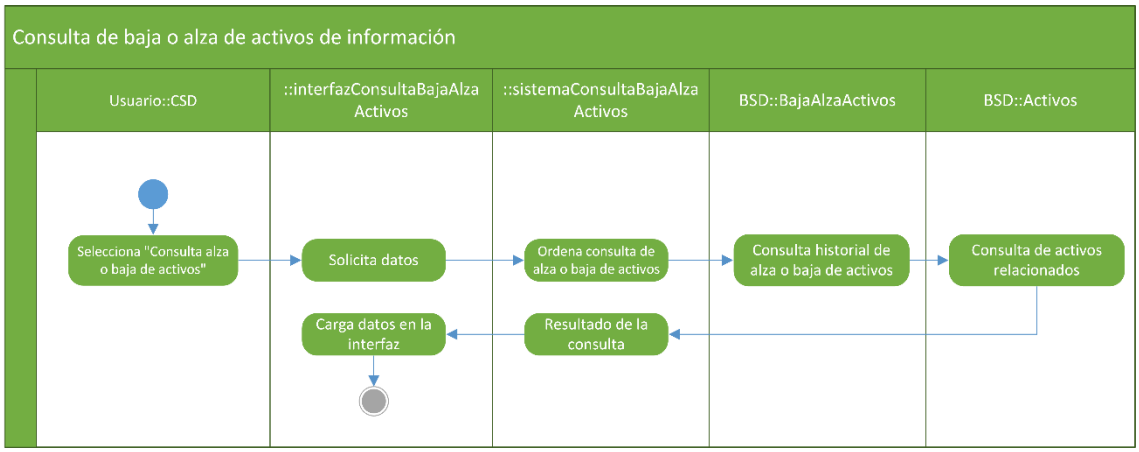

Ilustración 79: Consulta de registros de baja y alta de activos de información.
Fuente: Elaboración propia.

Gestión de riesgos y planes de tratamiento

La ilustración 80 representa el registro de un riesgo:

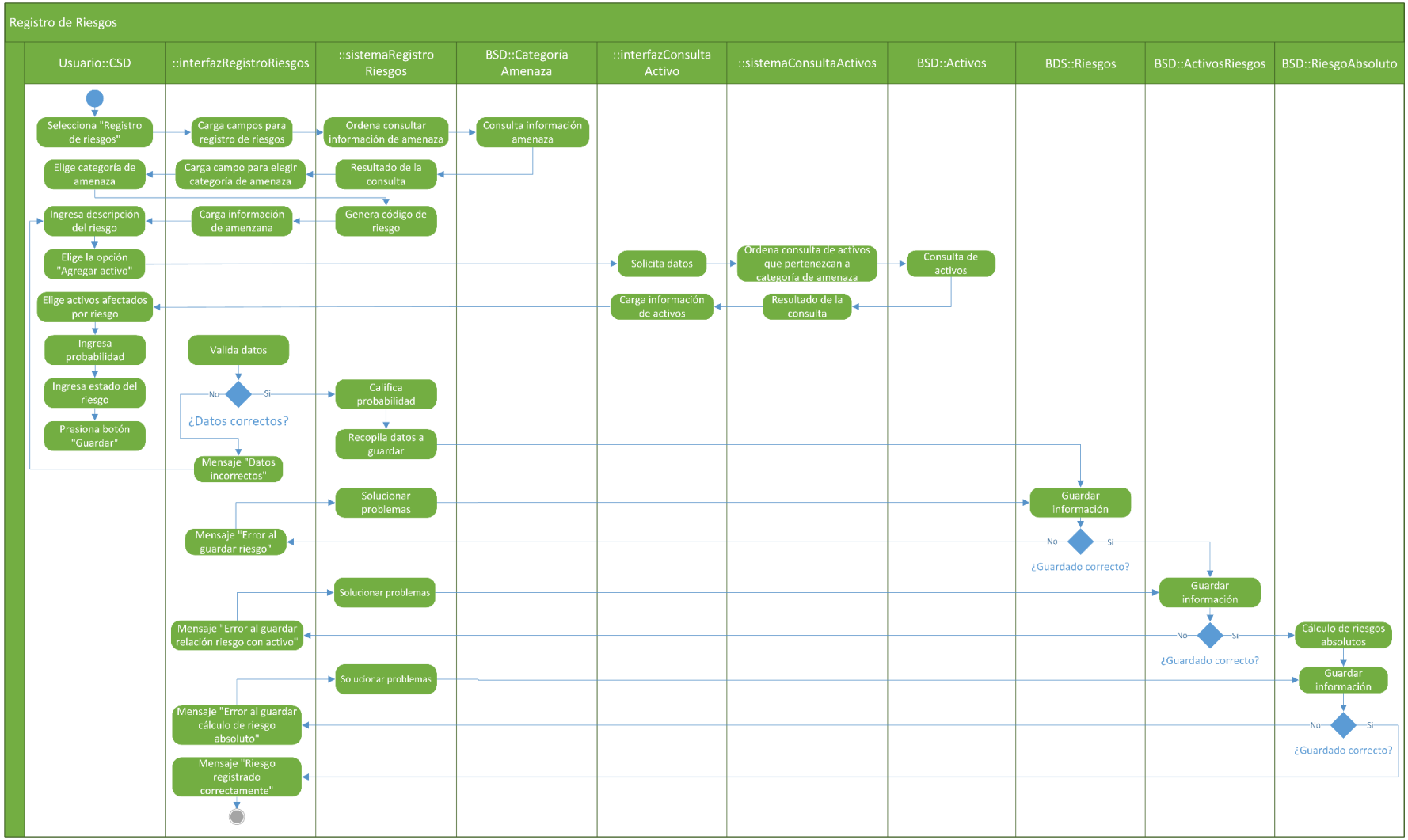

Ilustración 80: Registro de riesgo.
Fuente: Elaboración propia.

La ilustración 81 representa la consulta de los riesgos que han sido registrados en el sistema:

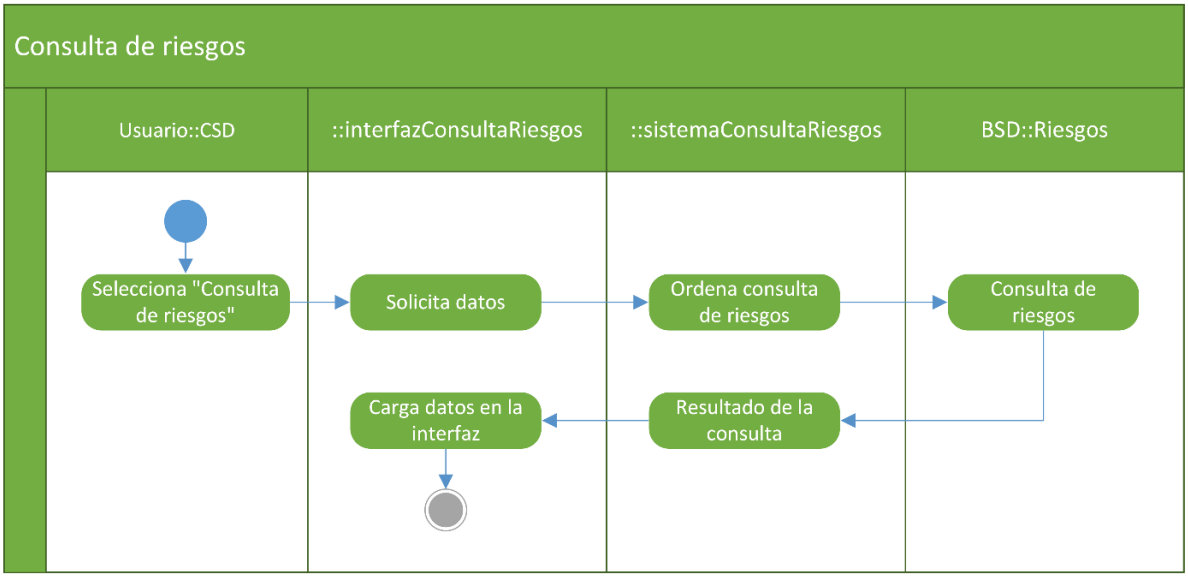

Ilustración 81: Consulta de riesgos.
Fuente: Elaboración propia.

La ilustración 82 representa la consulta detalle de un riesgo registrado en el sistema:

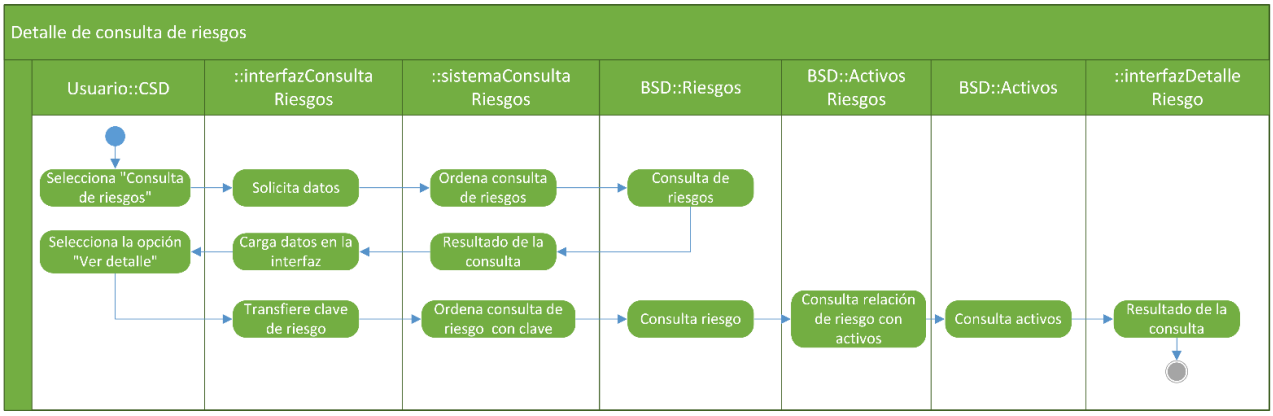

Ilustración 82: Detalle de una consulta de un riesgo.
Fuente: Elaboración propia.

La ilustración 83 representa la edición de información de un riesgo:

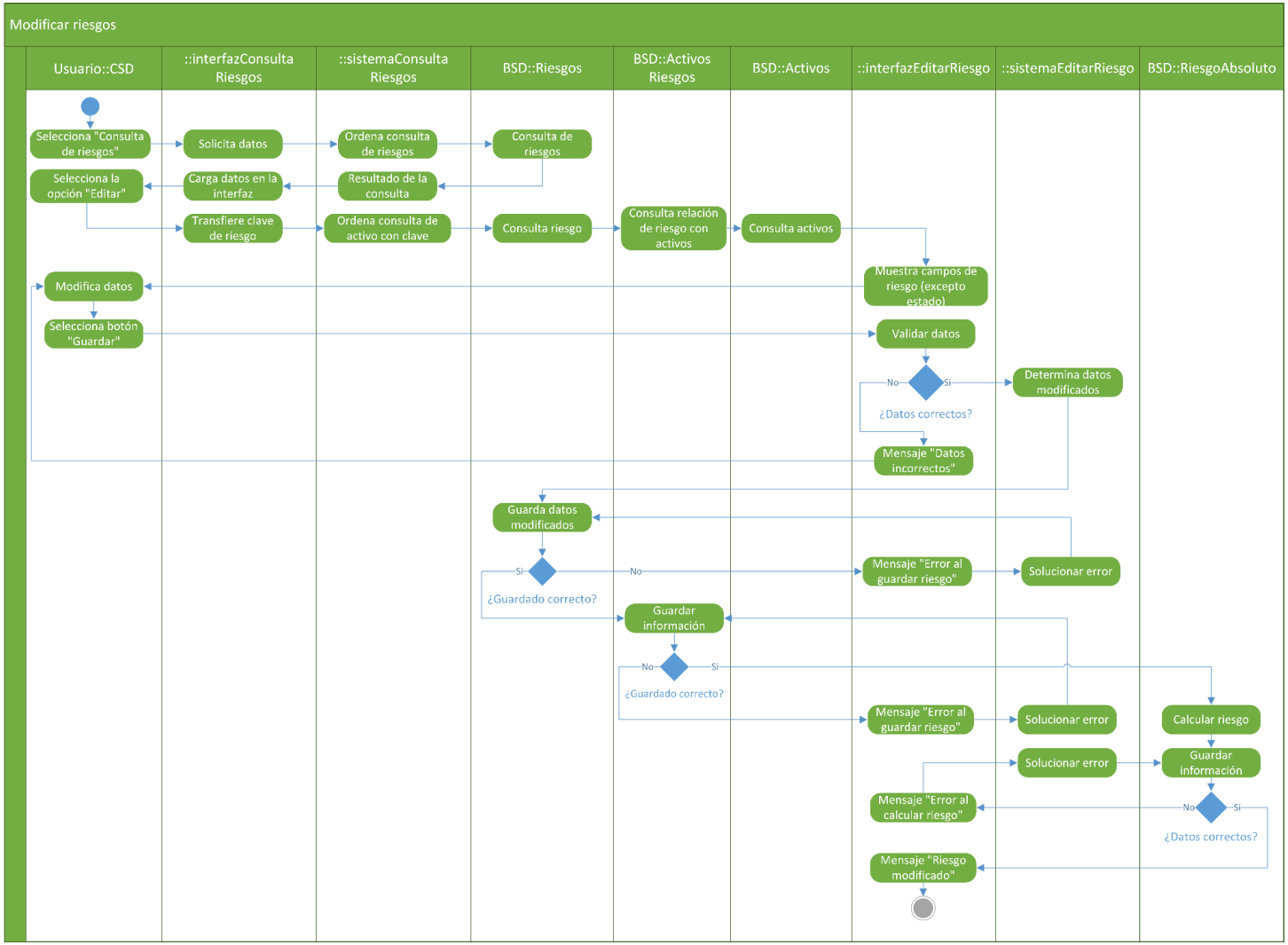

Ilustración 83: Edición de información de un riesgo.
Fuente: Elaboración propia.

La ilustración 84 representa la relación entre los activos con cada uno de sus riesgos registrados, además se muestra el cálculo del riesgo absoluto y acumulado:

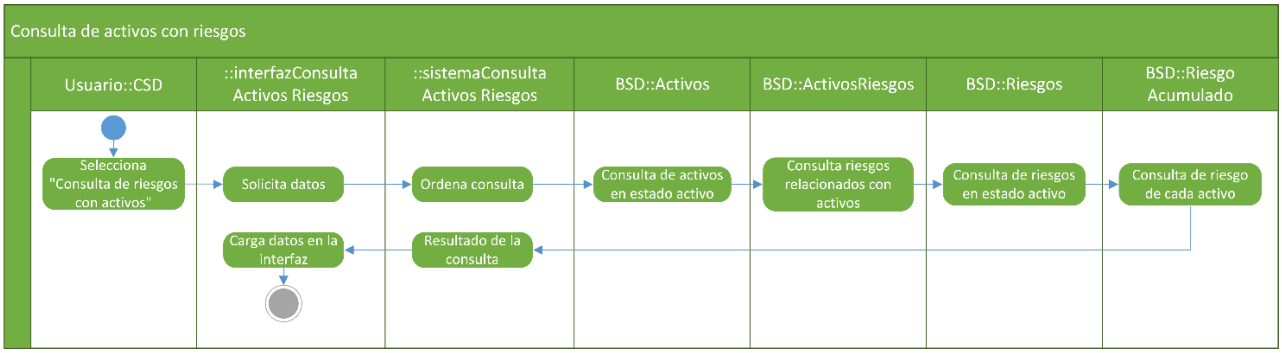

Ilustración 84: Relación entre activos y riesgos.
Fuente: Elaboración propia.

La siguiente ilustración 85 representa el registro de baja o registro de alta de un riesgo:

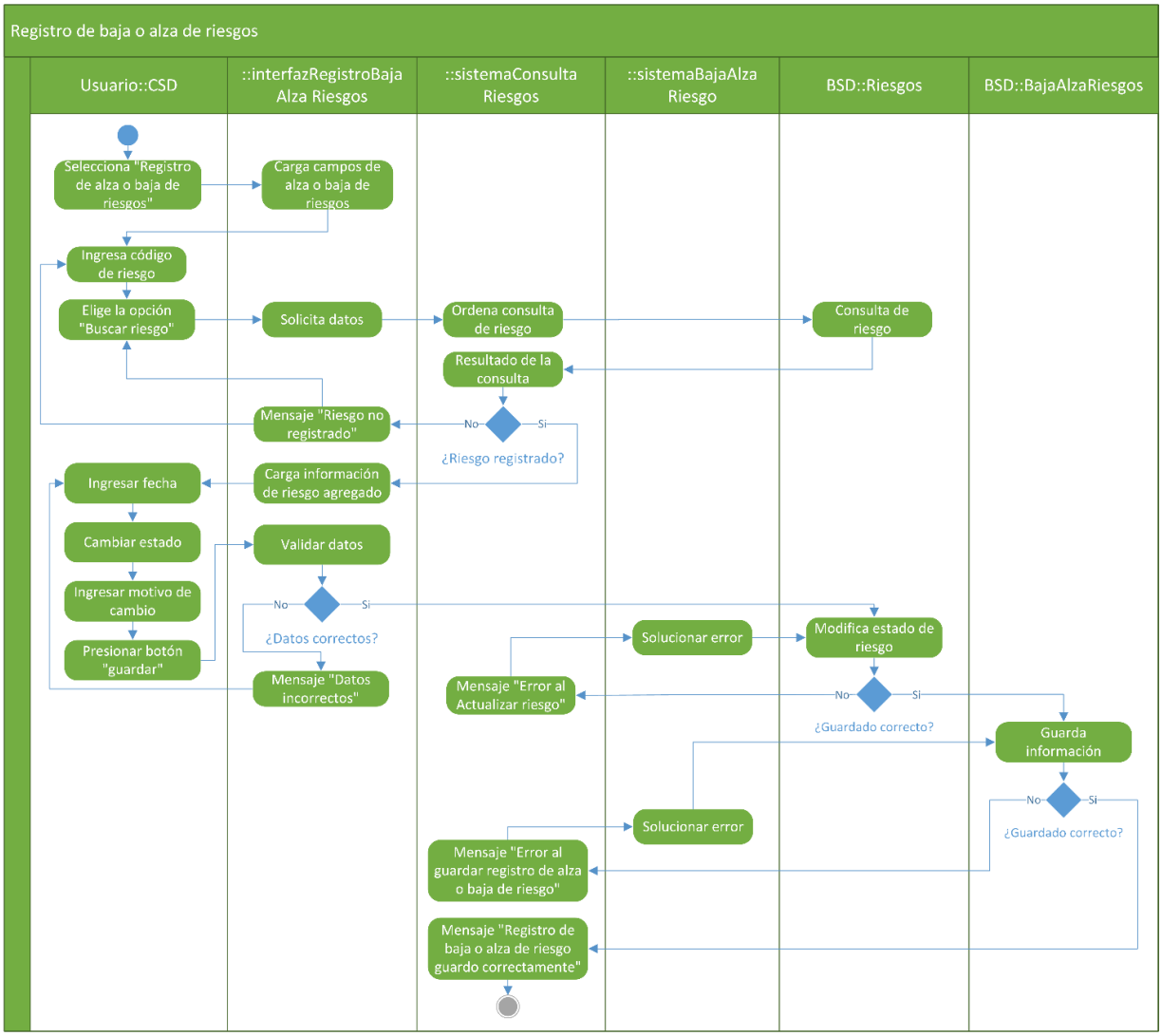

Ilustración 85: Registro de baja o alta de riesgo.
Fuente: Elaboración propia

La ilustración 86 representa la consulta de los registros de baja o alta de riesgos:

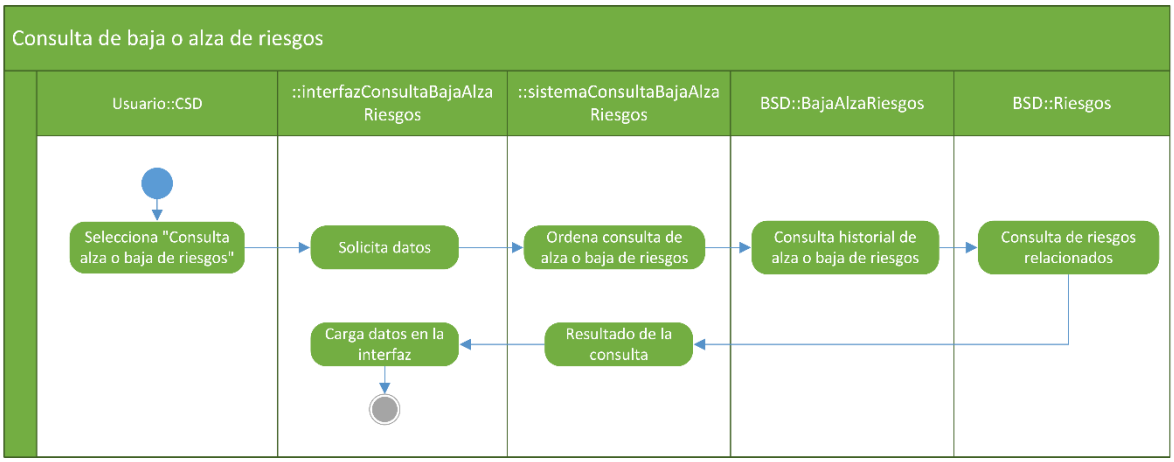

Ilustración 86: Consulta de registros de alta o baja de riesgos.
Fuente: Elaboración propia.

La ilustración 87 representa el registro de un plan de tratamiento que mitigue un riesgo:

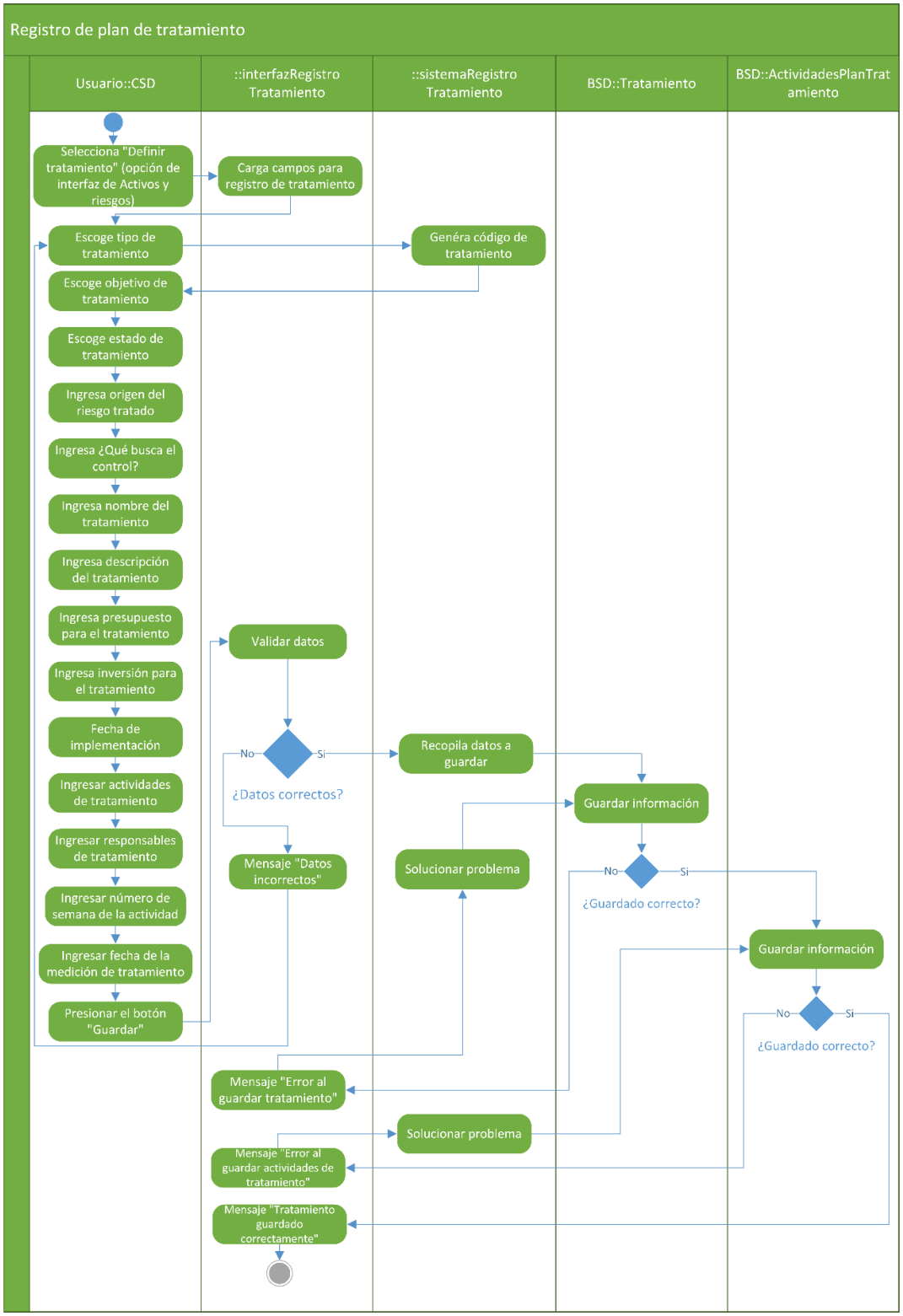

Ilustración 87: Registro de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 88 representa la consulta de los planes de tratamiento registrados en el sistema:

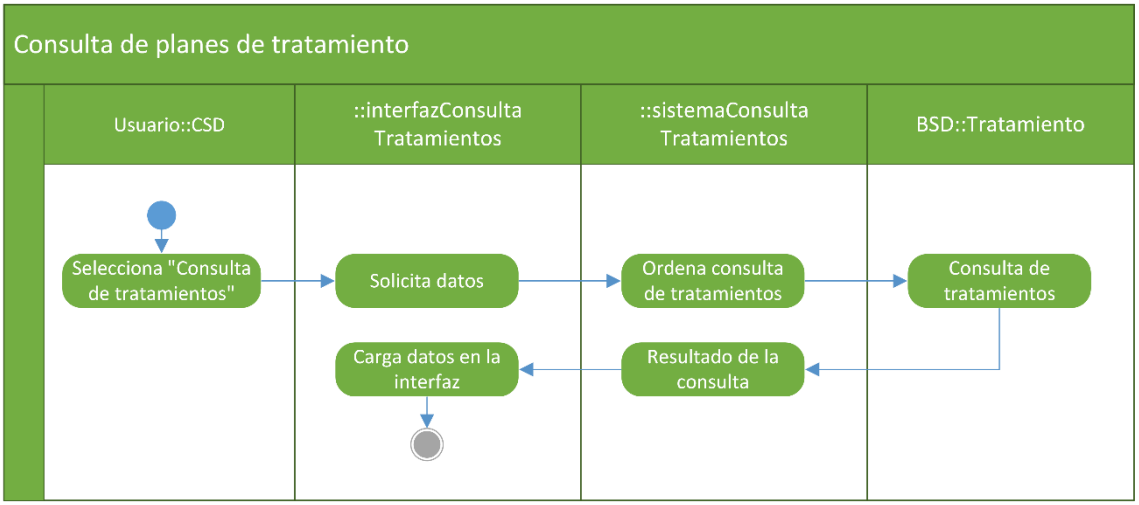

Ilustración 88: Consulta de planes de tratamiento.
Fuente: Elaboración propia.

La ilustración 89 representa la consulta detallada de un plan de tratamiento registrados en el sistema:

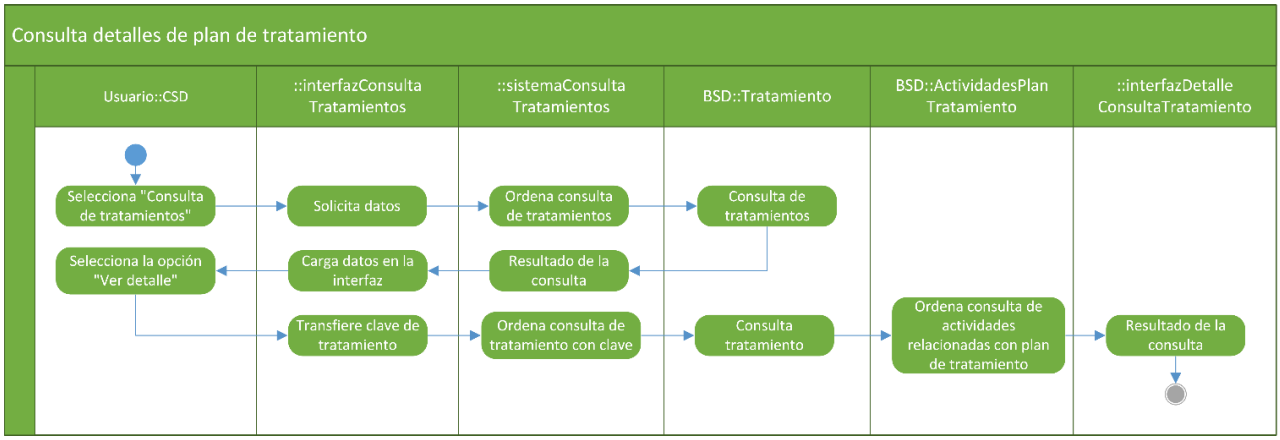

Ilustración 89: Consulta de detalles de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 90 representa la edición de información de un plan de tratamiento registrado en el sistema:

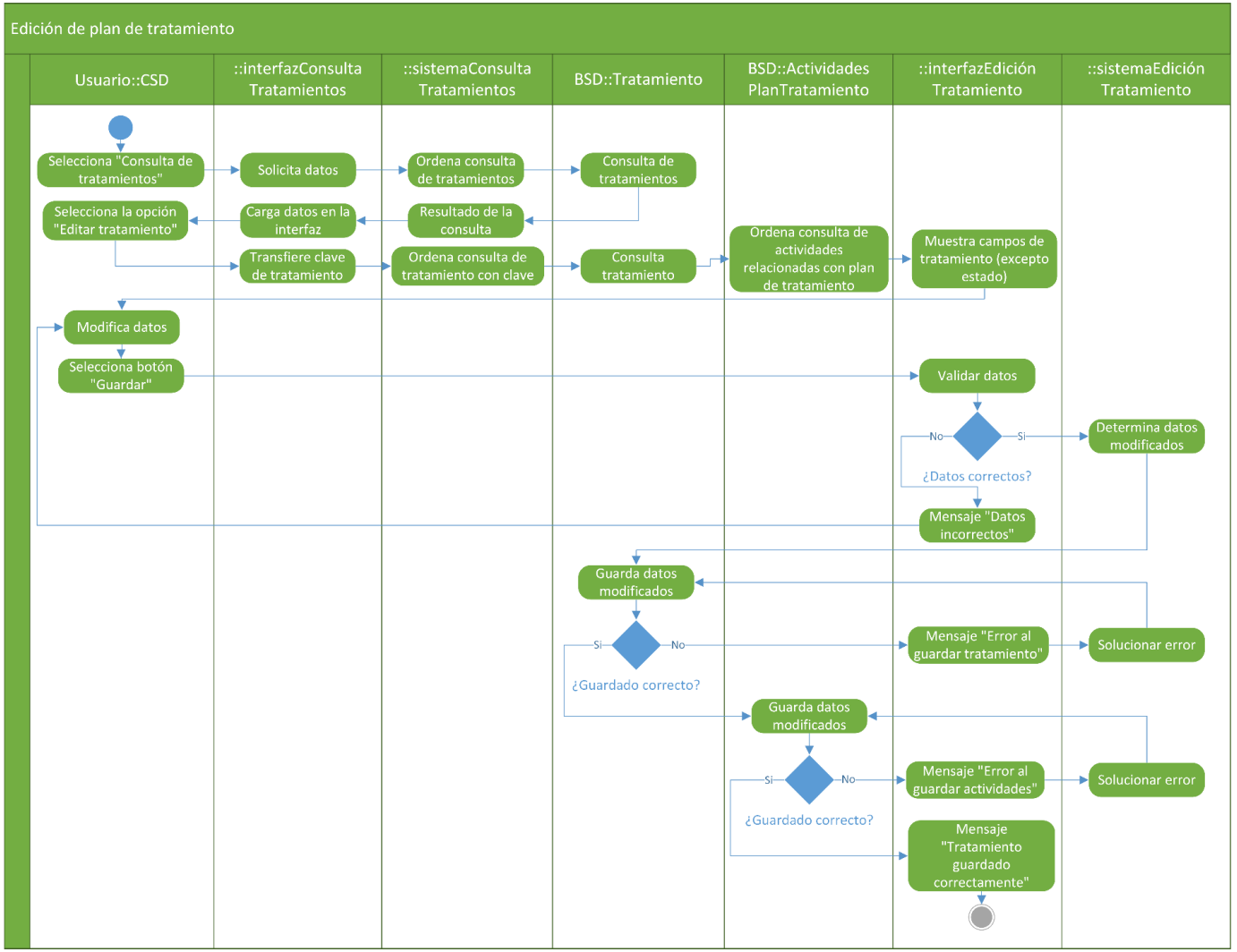

Ilustración 90: Edición de información de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 91 representa la edición de información de un plan de tratamiento registrado en el sistema:

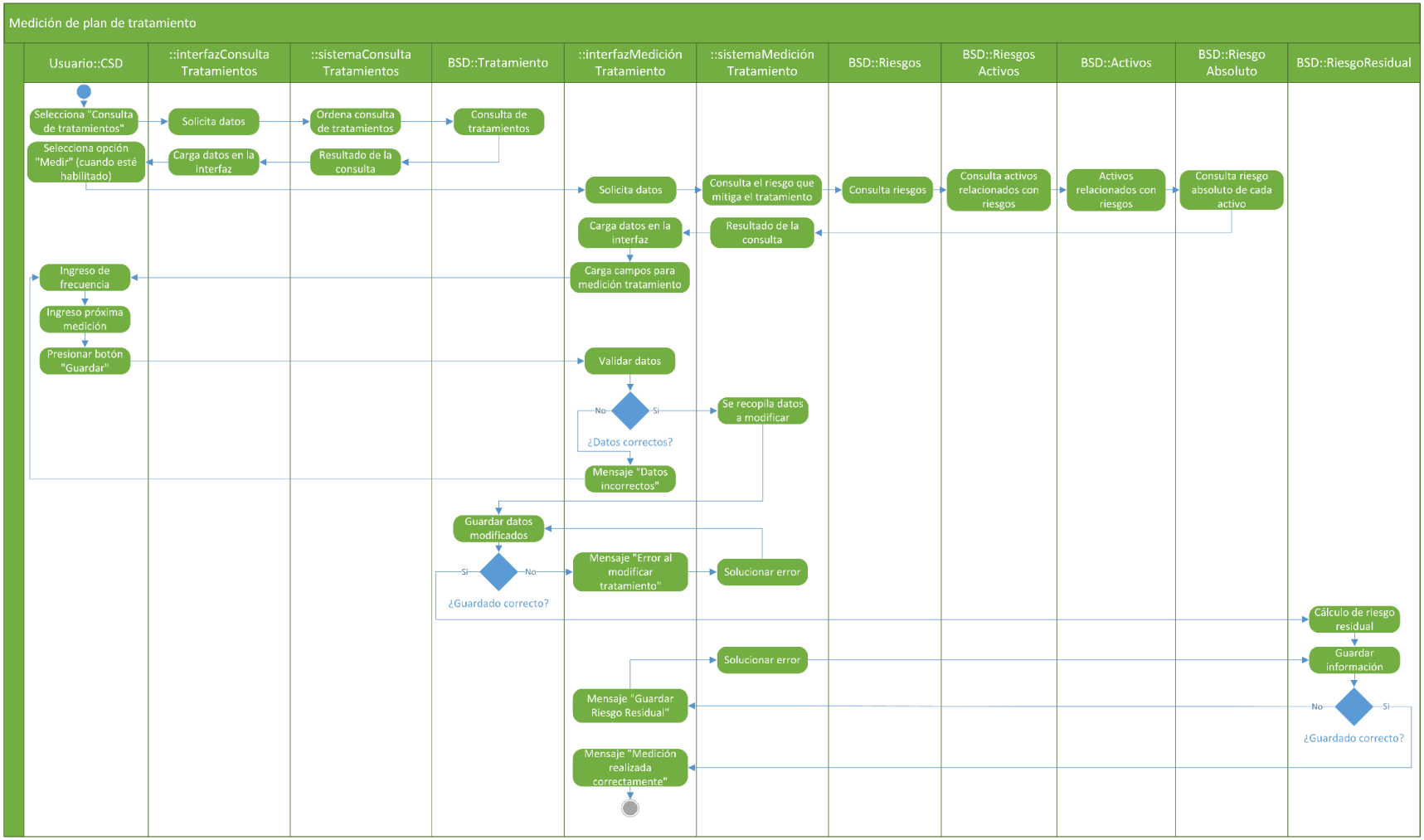

Ilustración 91:Medición de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 92 representa el registro de baja o registro de alta de un plan de tratamiento:

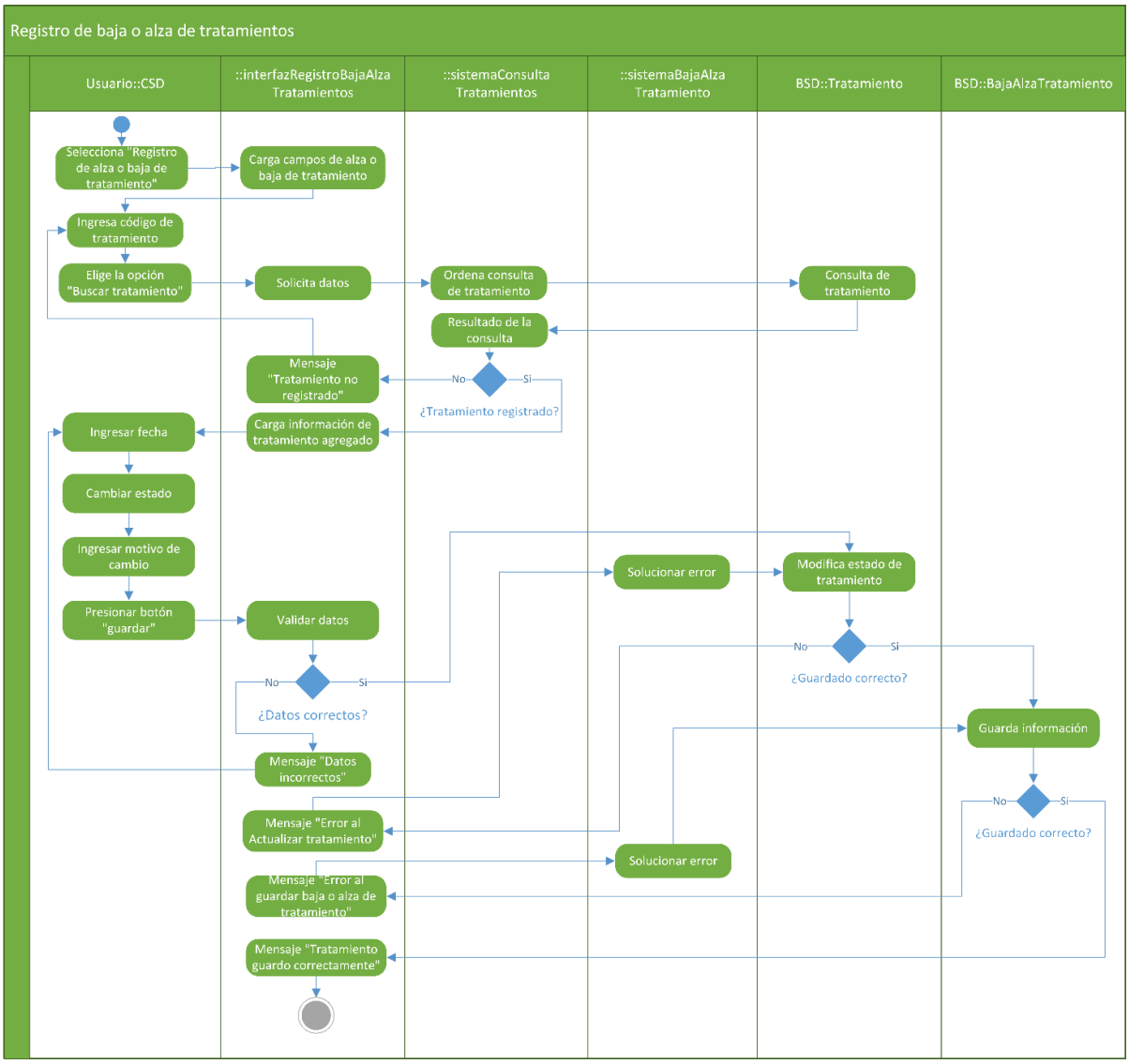

Ilustración 92: Registro de baja o alta de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 93 representa la consulta de los registros de baja o alta de planes de tratamiento.

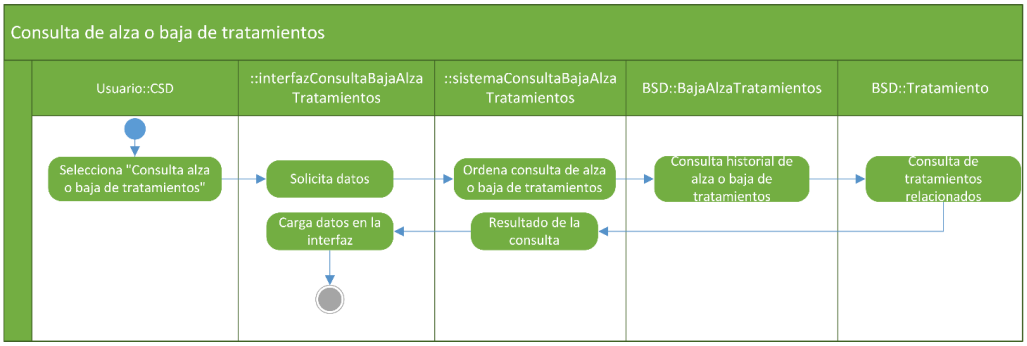

Ilustración 93:Consulta de registros de baja o alta de planes de tratamiento.
Fuente: Elaboración propia.

La ilustración 94 representa la consulta de la relación entre los activos, cada riesgos y tratamiento que mitiga dicho riesgo, así mismo se muestra el riesgo absoluto y acumulado del riesgo, como también el riesgo residual del tratamiento:

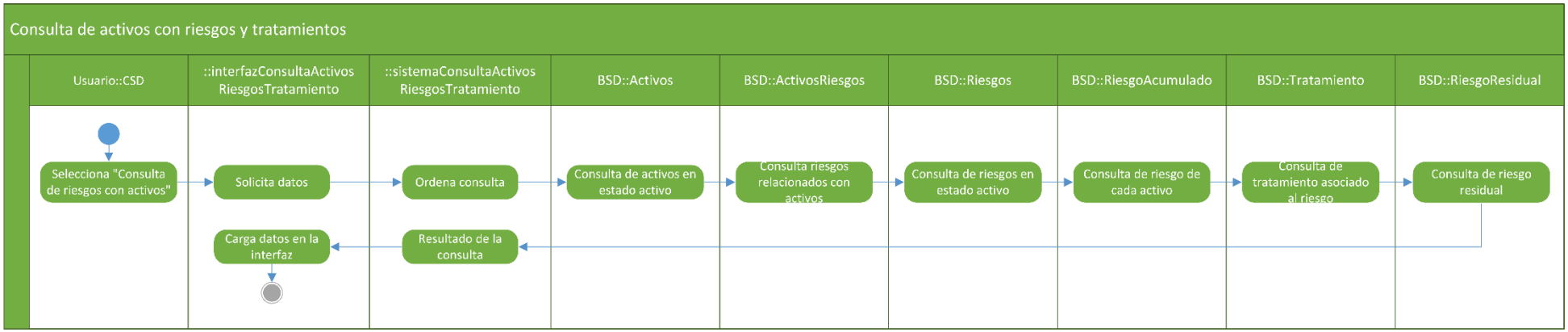

Ilustración 94: Relación activos con riesgos y plantes de tratamiento.
Fuente: Elaboración propia.

Gestión de incidentes

La ilustración 95 representa el registro de incidentes suscitados dentro de la empresa:

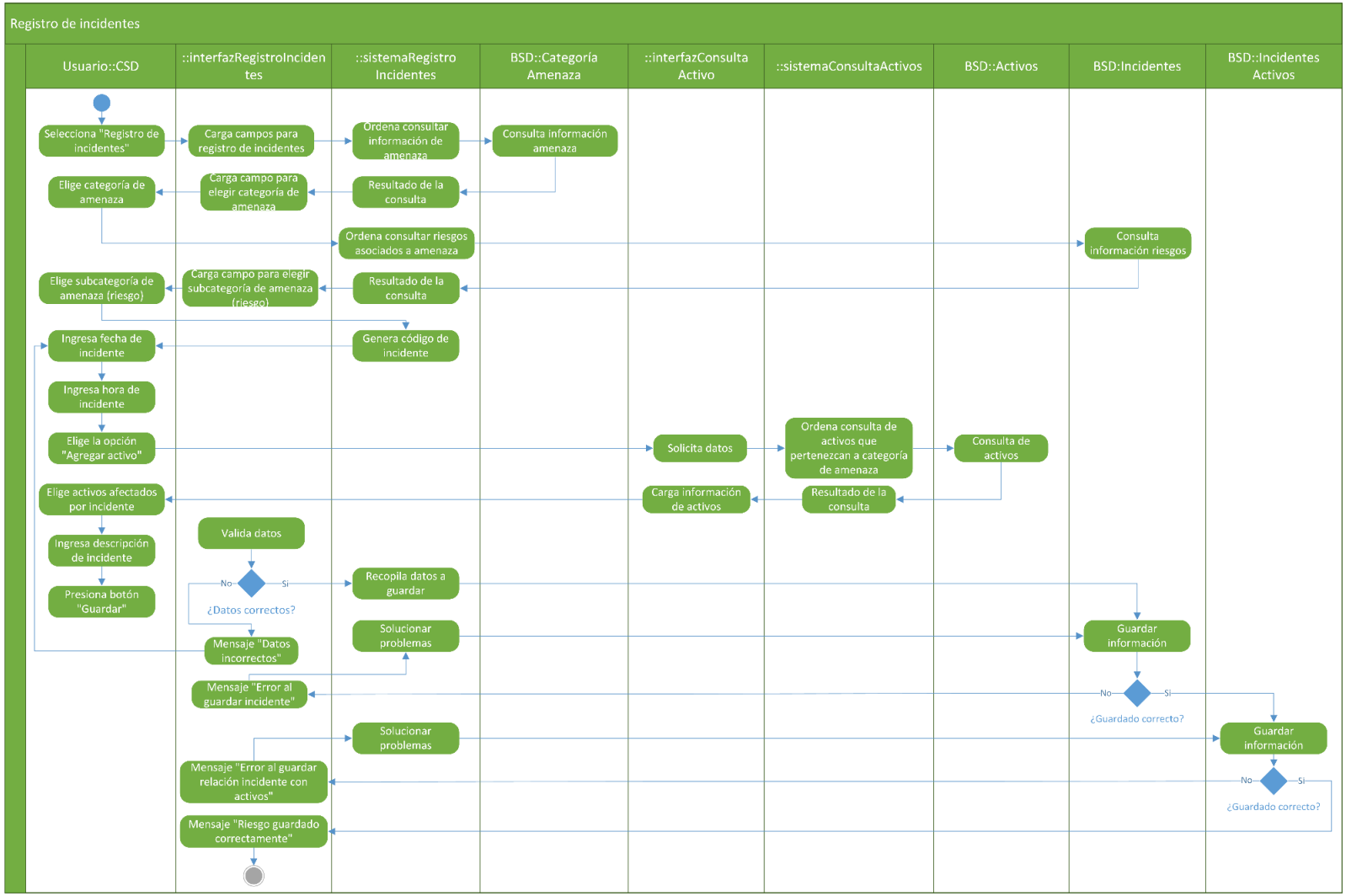

Ilustración 95: Registro de incidentes.
Fuente: Elaboración propia.

La ilustración 96 representa la consulta de los incidentes que hayan sido registrados en el sistema:

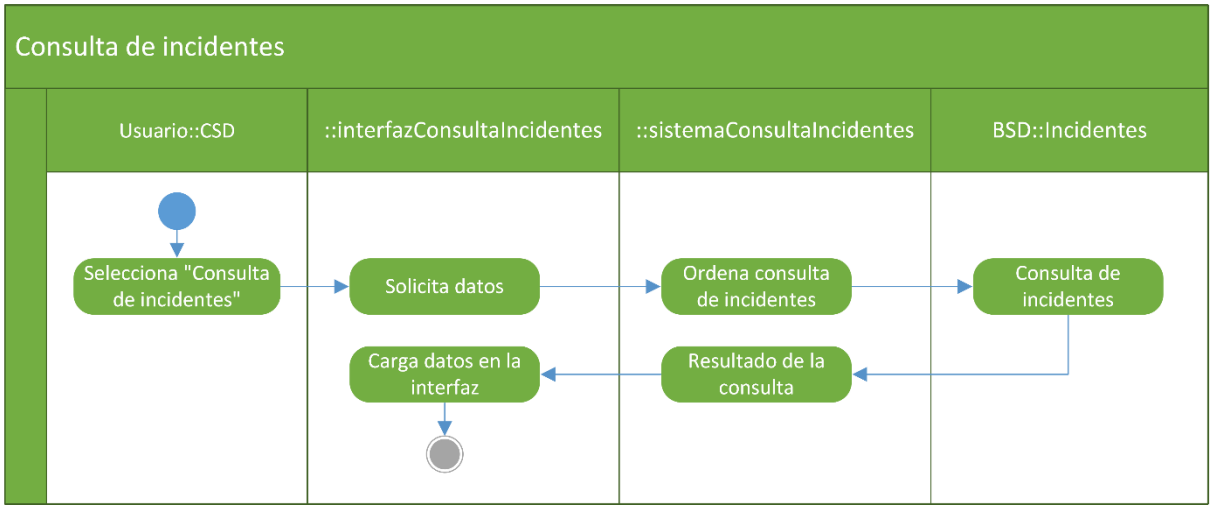

Ilustración 96: Consulta de registro de incidentes.
Fuente: Elaboración propia.

La ilustración 97 representa la consulta de los detalles de un incidente que hayan sido registrado en el sistema:

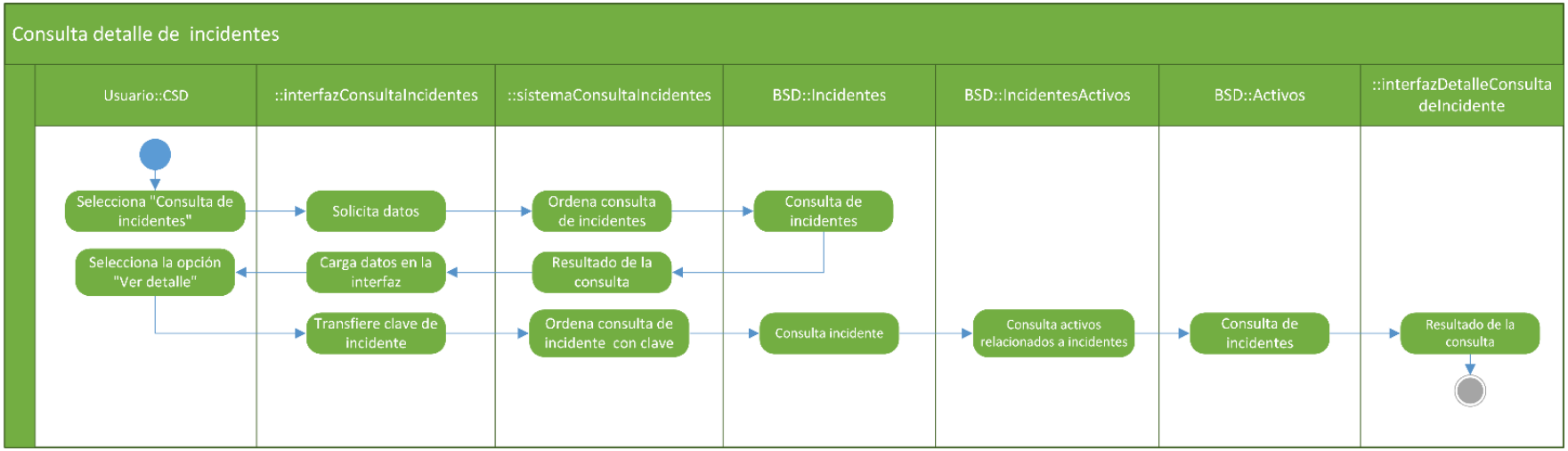

Ilustración 97: Consulta de detalles de incidente registrado.
Fuente: Elaboración propia.

La ilustración 98 la edición de información de un incidente:

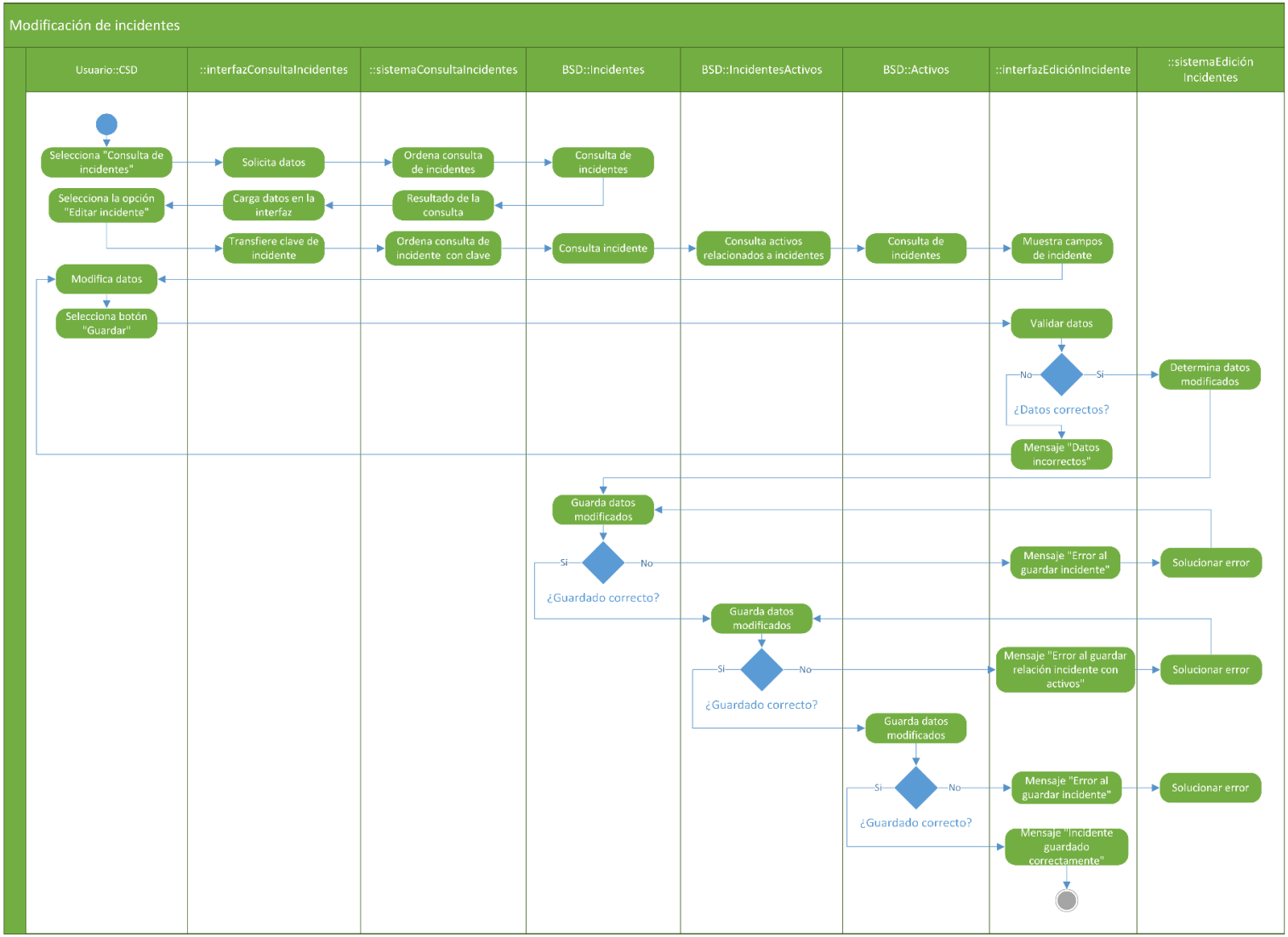

Ilustración 98: Edición de información de un incidente.
Fuente: Elaboración propia.

Gestión de procesos de negocio

La ilustración 99 representa el registro de un proceso de negocio de la organización en el sistema:

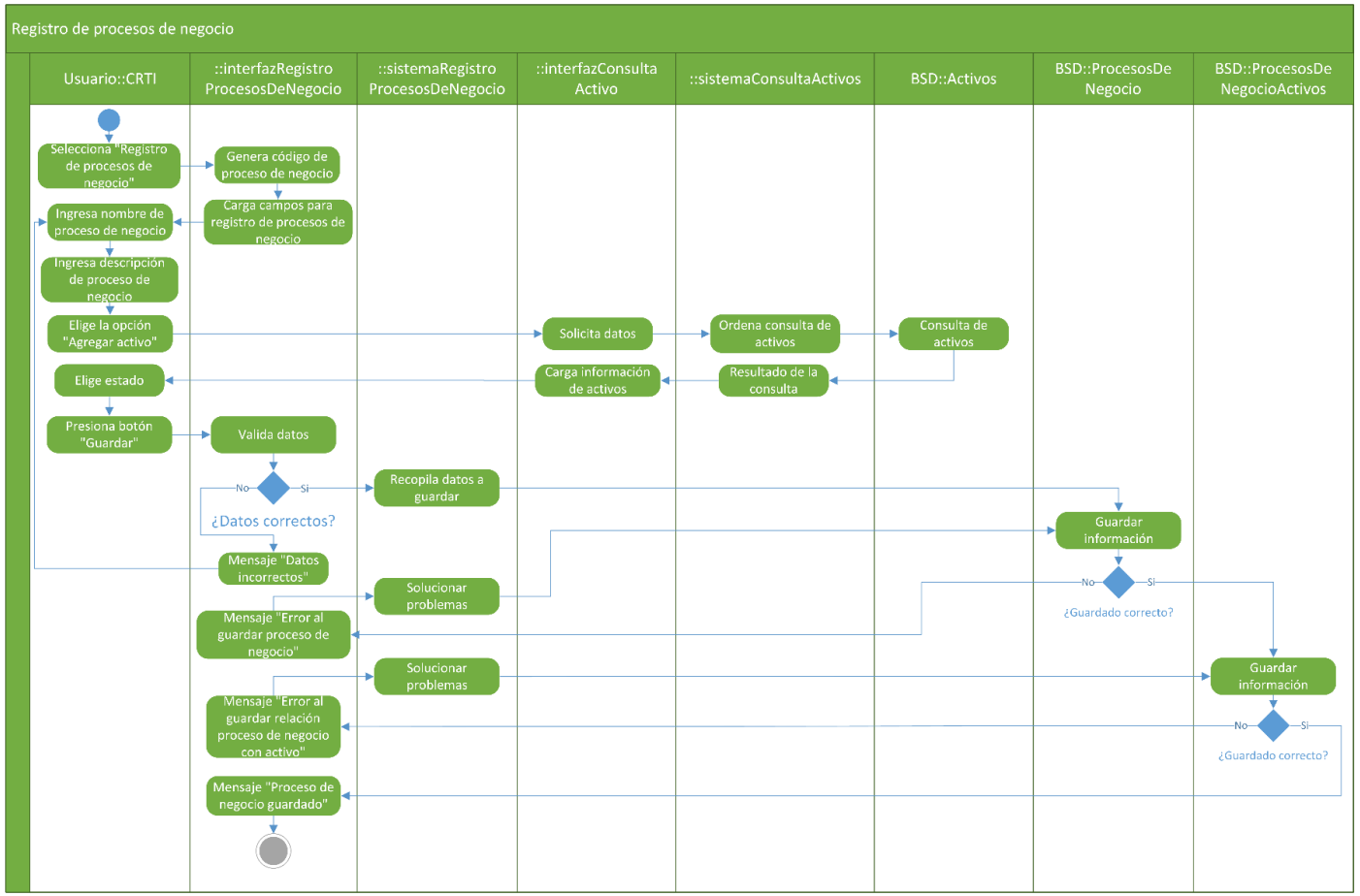

Ilustración 99: Registro de procesos de negocio.
Fuente: Elaboración propia.

La ilustración 100 representa la consulta de los procesos de negocio que hayan sido registrados en el sistema:

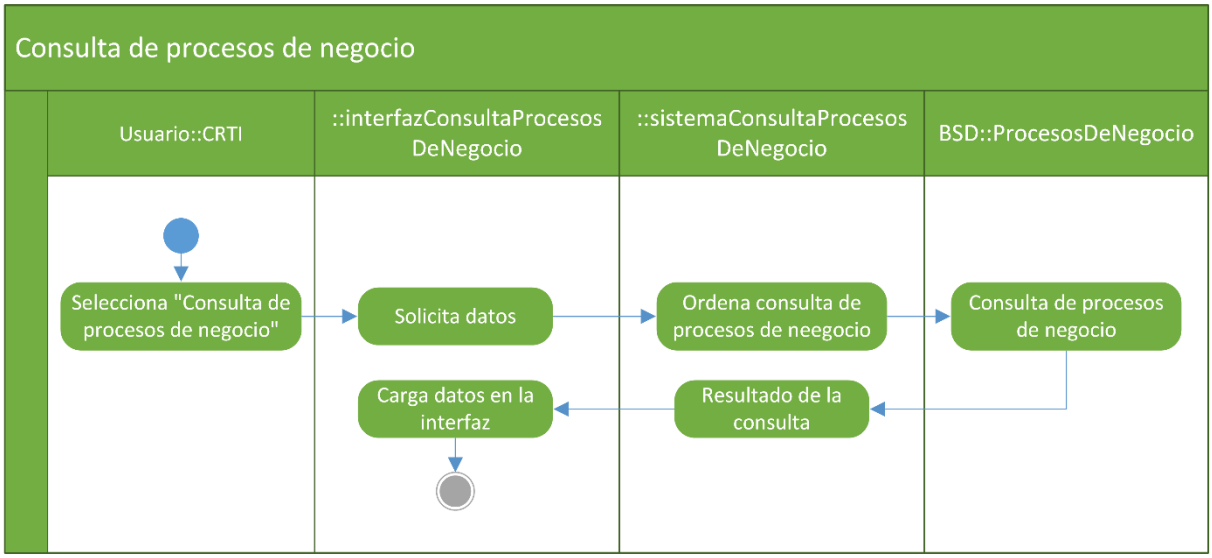

Ilustración 100: Consulta de procesos de negocio.
Fuente: Elaboración propia.

La ilustración 101 representa los detalles de la consulta de un proceso de negocio:

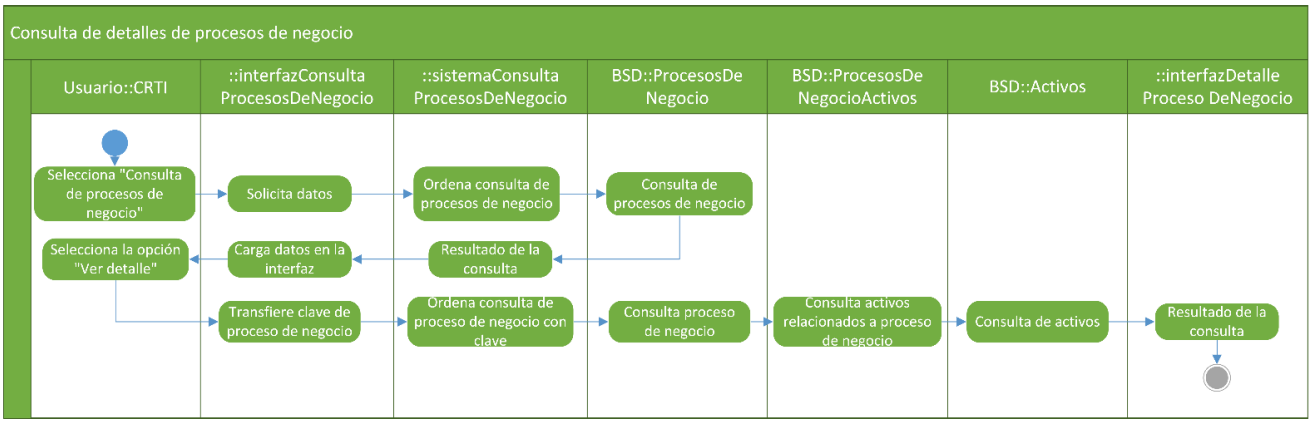

Ilustración 101: Consulta de detalles de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 102 representa la edición de información de un proceso de negocio:

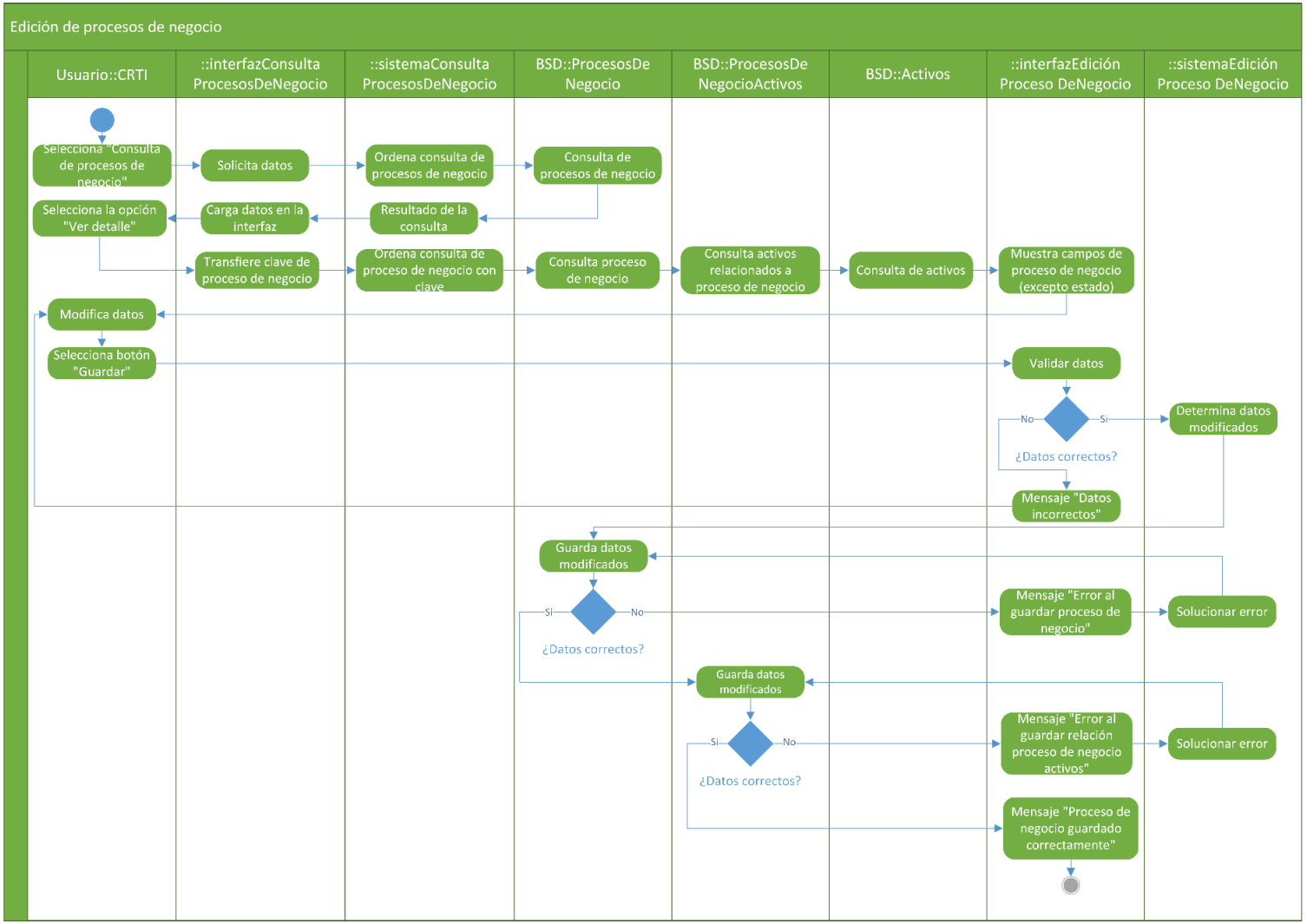

Ilustración 102: Edición de información de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 103 representa el registro de baja o registro de alta de un proceso de negocio que haya sido registrado en el sistema:

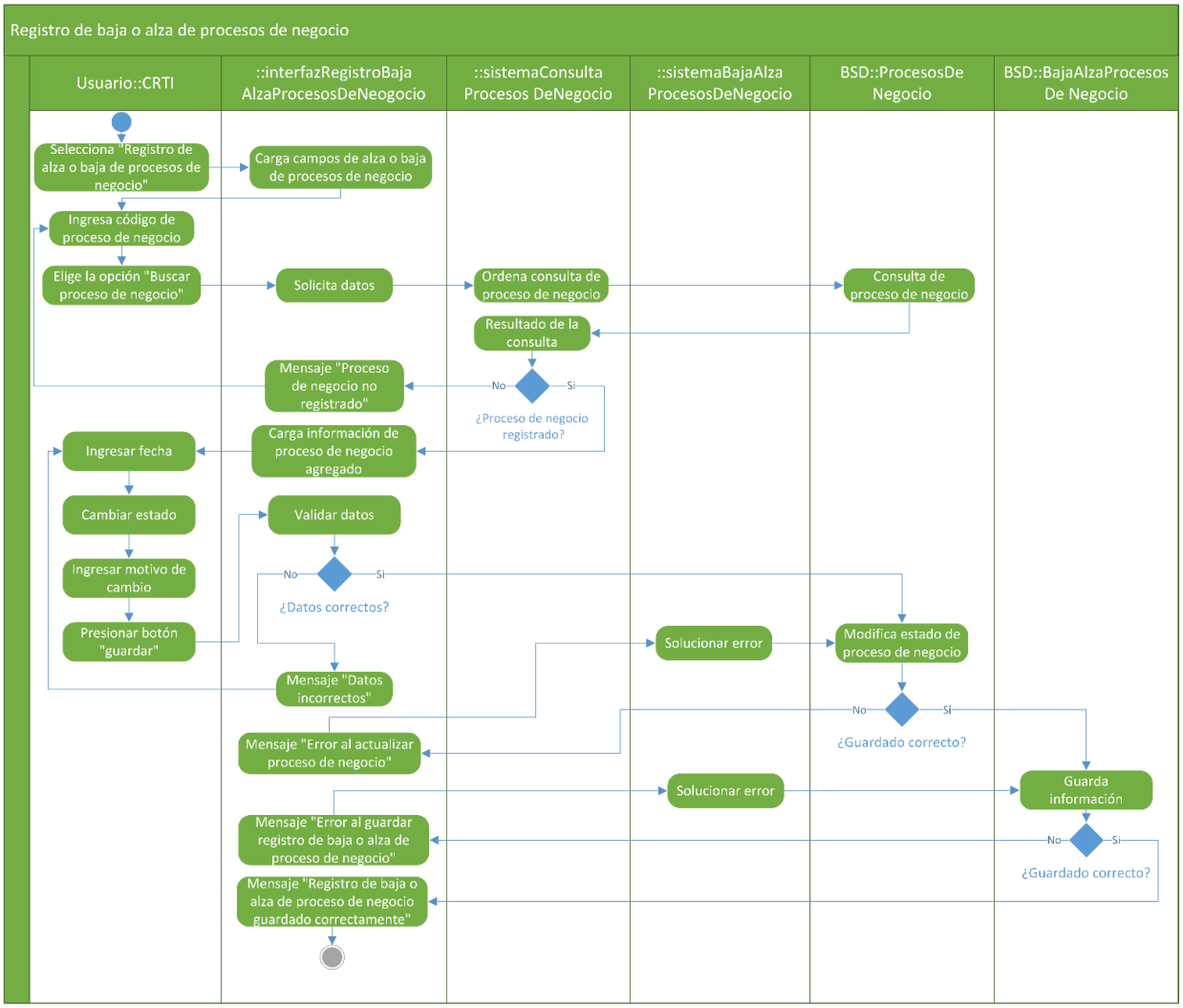

Ilustración 103: Registro de baja o alta de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 104 representa la consulta de los registros de baja o alta de procesos de negocio:

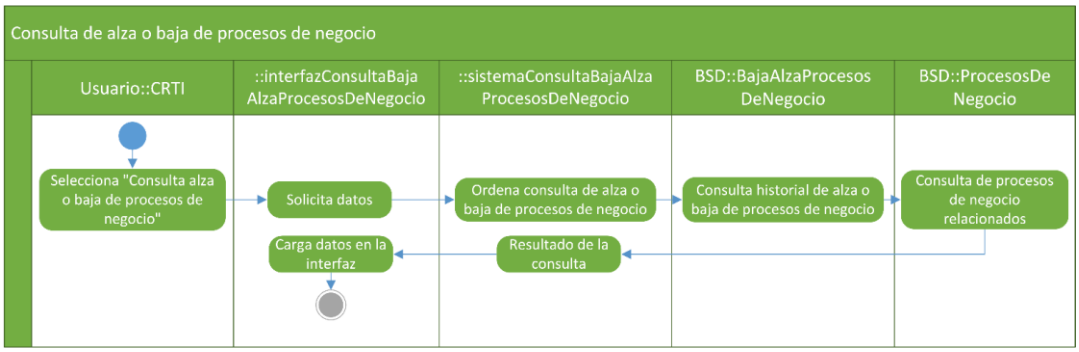

Ilustración 104: Consulta de baja o alta de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 105 representa el registro de incidentes a procesos de negocio, ya que si un proceso de negocio es reportado se le debe dar un seguimiento:

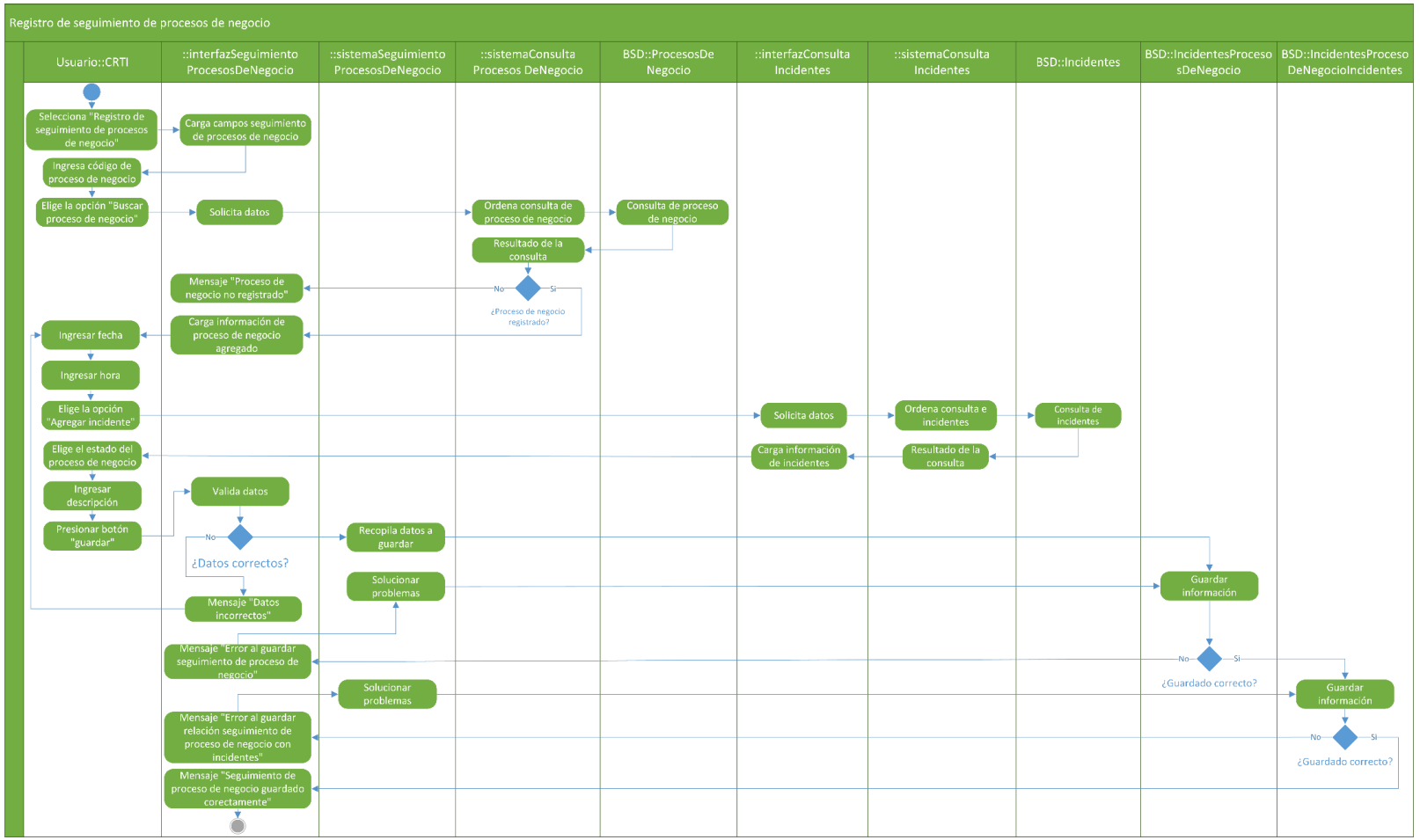

Ilustración 105: Registro de seguimiento de un proceso de negocio.
Fuente: Elaboración propia.

La ilustración 106 representa la consulta de los procesos de negocio que hayan sido reportando con algún incidente:

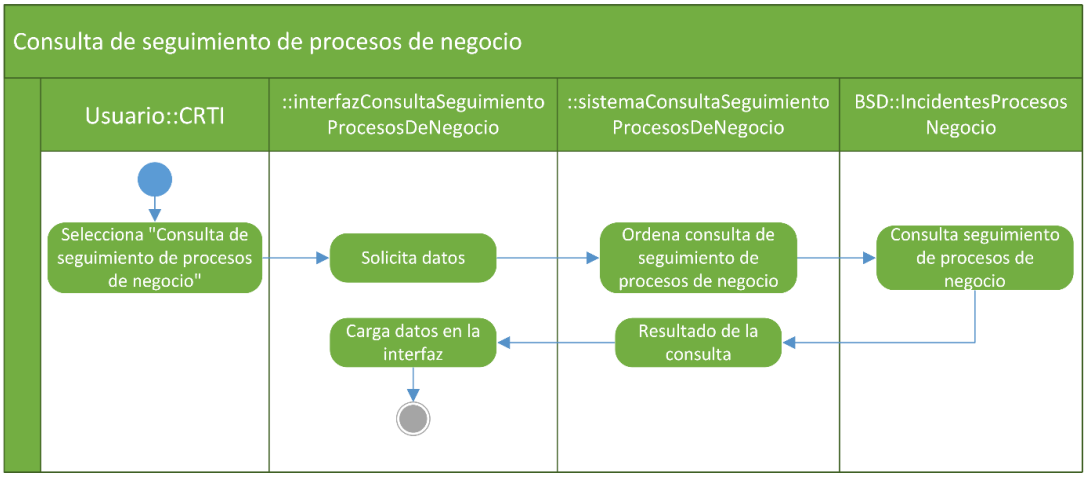

Ilustración 106: Consulta de seguimiento de procesos de negocio.
Fuente: Elaboración propia.

La ilustración 107 representa la consulta la de los detalles de un proceso de negocio en seguimiento, que ha sido registrado en el sistema:

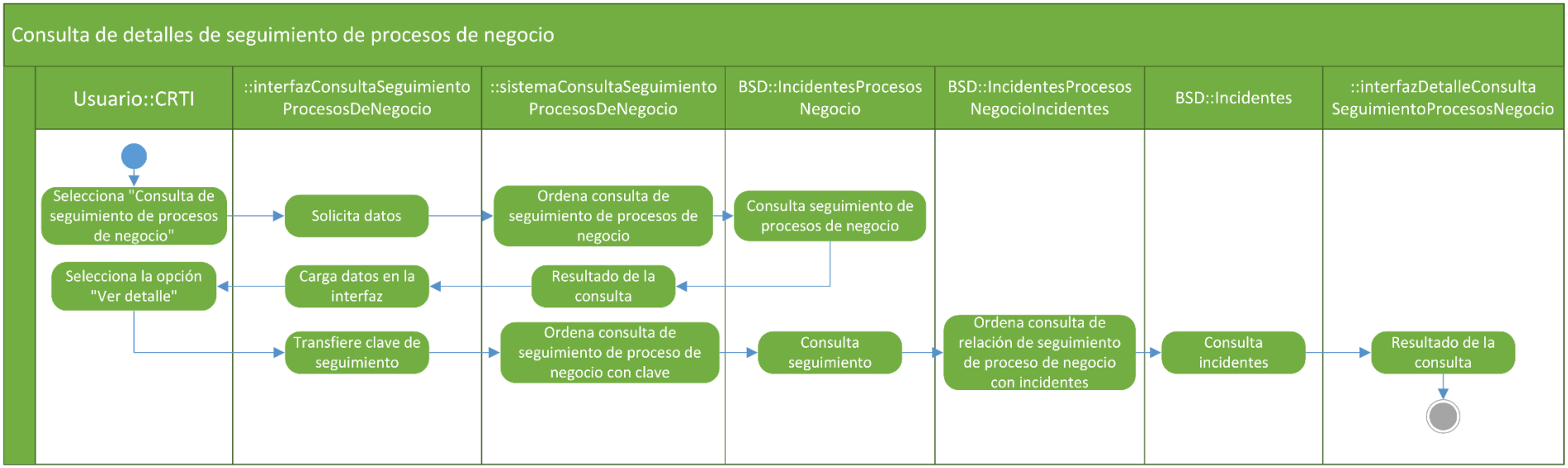

Ilustración 107: Consulta de detalles de un proceso de negocio en seguimiento.
Fuente: Elaboración propia.

La 108, representa la edición de información de un seguimiento de proceso de negocio que haya sido registrado en el sistema:

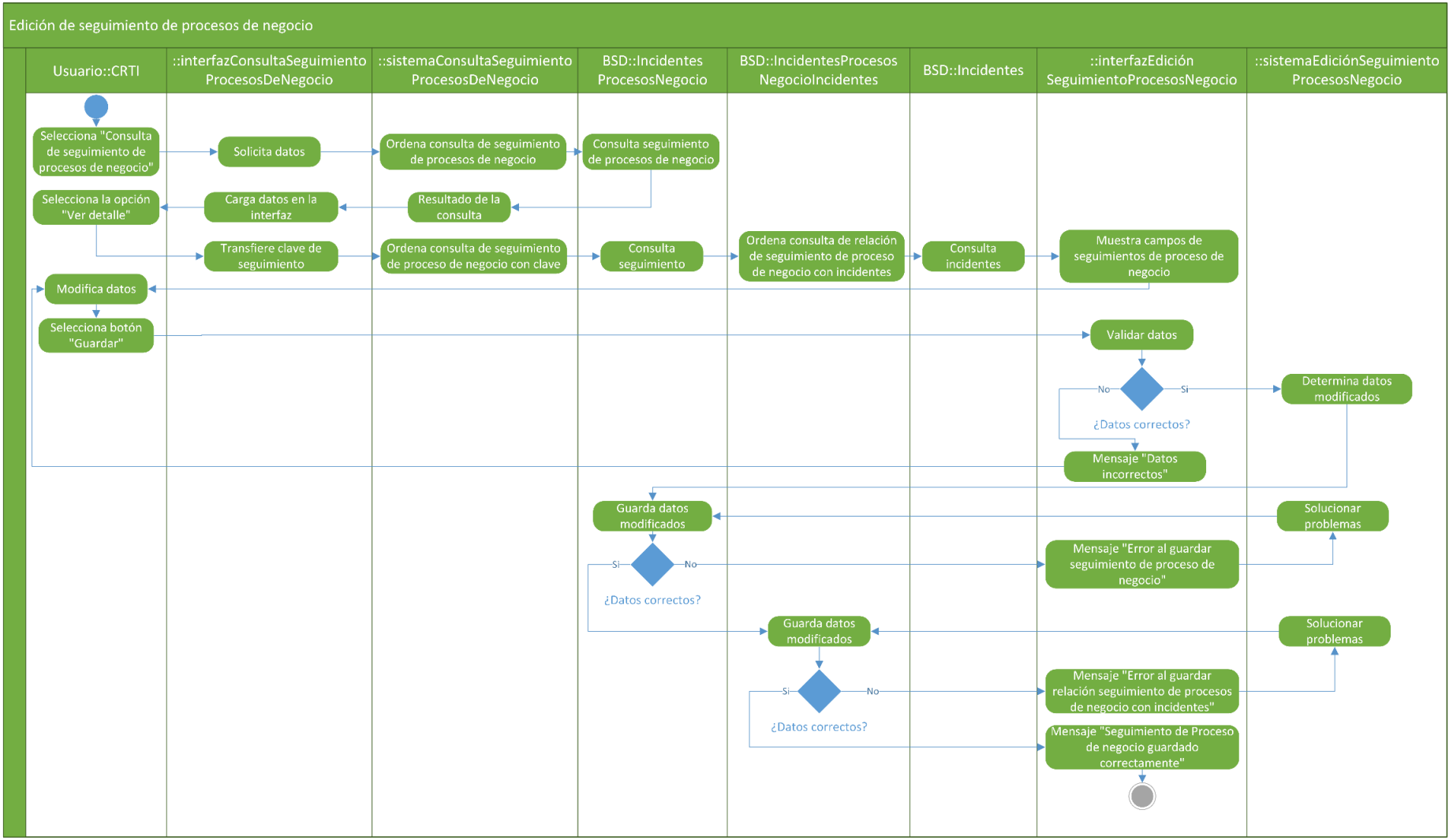

Ilustración 108: Edición de información de seguimiento de procesos de negocio.
Fuente: Elaboración propia.

Reportes

La ilustración 109 representa los reportes de indicadores clave de desempeño de incidentes registrados en el sistema:

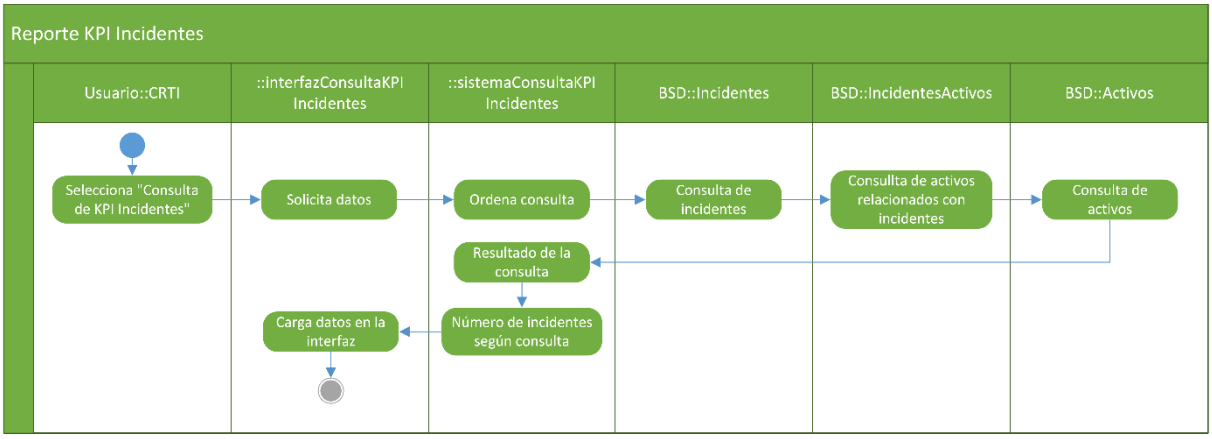

Ilustración 109: Reporte de indicadores clave de desempeño de incidentes.
Fuente: Elaboración propia.

La ilustración 110 representa los reportes de indicadores clave de desempeño de procesos de negocio:

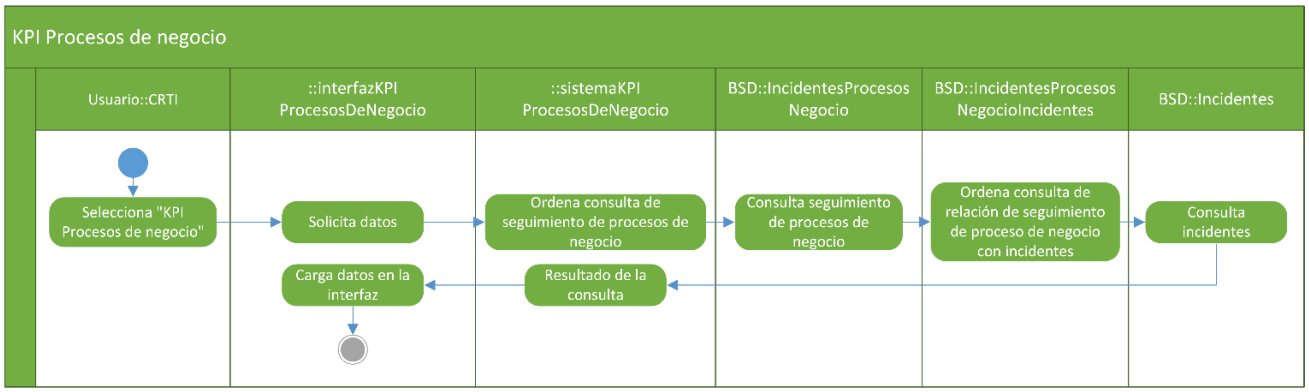

Ilustración 110: Reporte de indicadores clave de desempeño de procesos de negocio.
Fuente: Elaboración propia.

La ilustración 111 representa los reportes de indicadores clave de desempeño de planes de tratamiento:

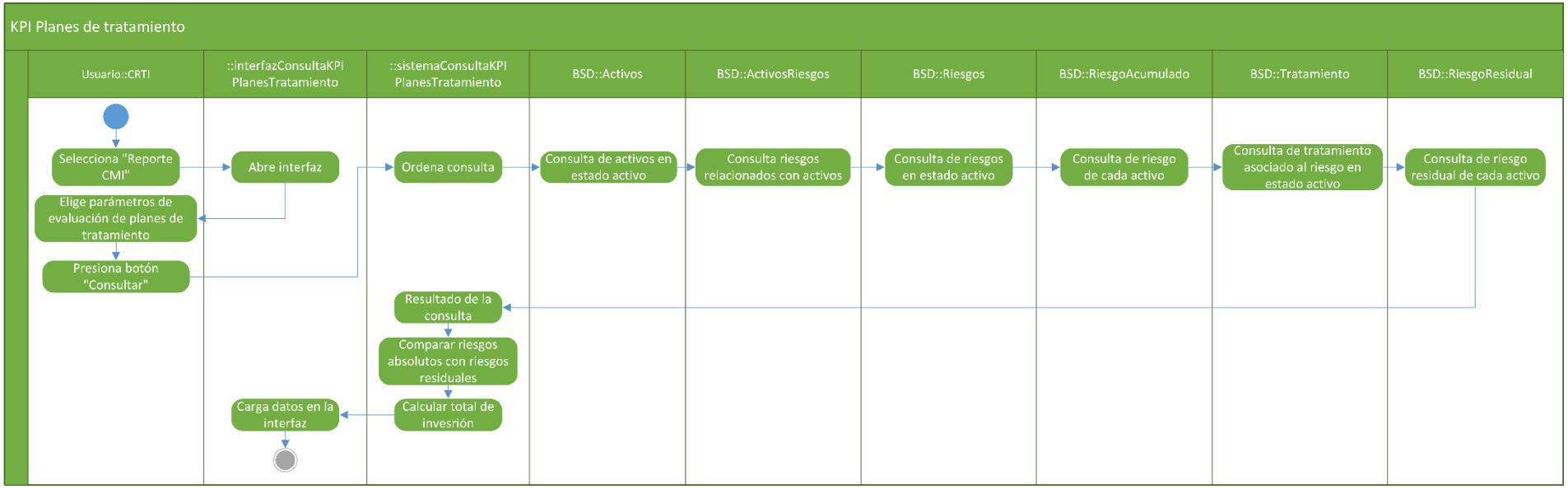

Ilustración 111: Reporte de indicadores clave de desempeño de planes de tratamiento.
Fuente: Elaboración propia.

La ilustración 112 representa un reporte de cuadro de mando integrado (CMI), en donde, se relaciona cada proceso de negocio y todos sus activos que lo componen; con cada activo se muestran los riesgos que tiene cada uno, también el tratamiento registrado que lo mitiga (si lo tiene), como información adicional se muestra n los riesgos absolutos y residuales de cada uno:

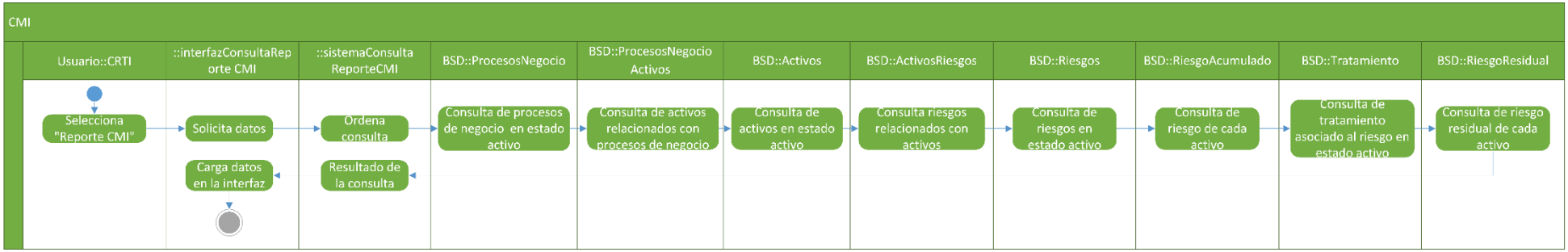

Ilustración 112: Reporte de cuadro de mando integrado.
Fuente: Elaboración propia

Gestión de usuario

La ilustración 113 representa el registro de un usuario del sistema:

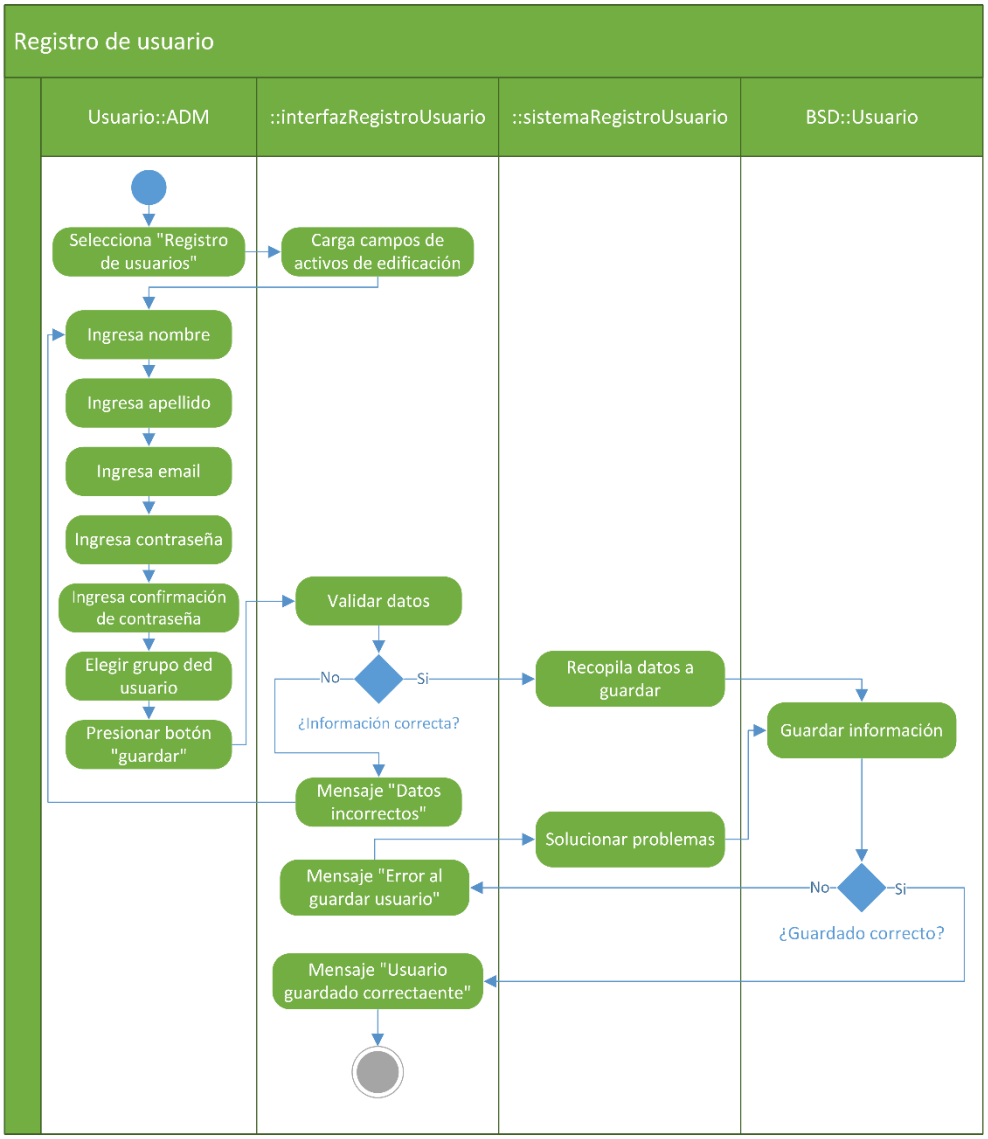

Ilustración 113: Registro de usuarios.
Fuente: Elaboración propia.

La ilustración 114 representa la consulta de los usuarios registrados en el sistema:

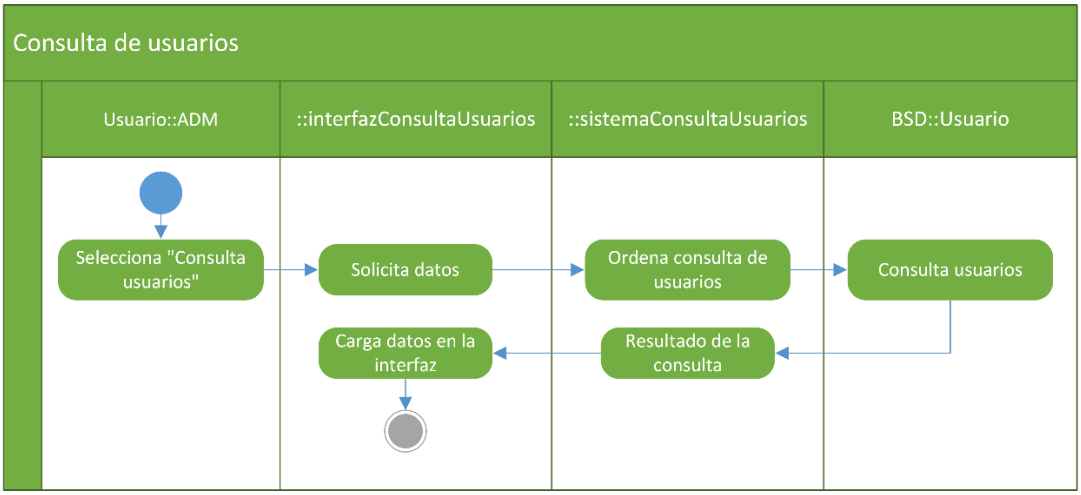

Ilustración 114: Consulta de usuarios registrados en el sistema.
Fuente: Elaboración propia.

La ilustración 115 representa la consulta de los detalles de un usuario registrado en el sistema:

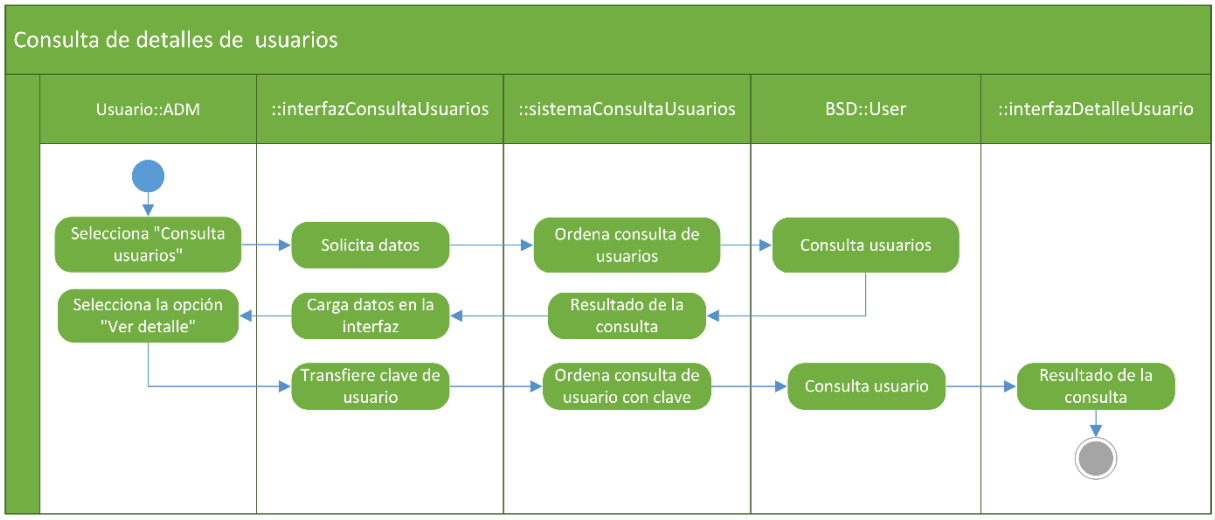

Ilustración 115: Consulta de detalles de un usuario.
Fuente: Elaboración propia.

La ilustración 116 representa la edición de información de los usuarios registrados en el sistema:

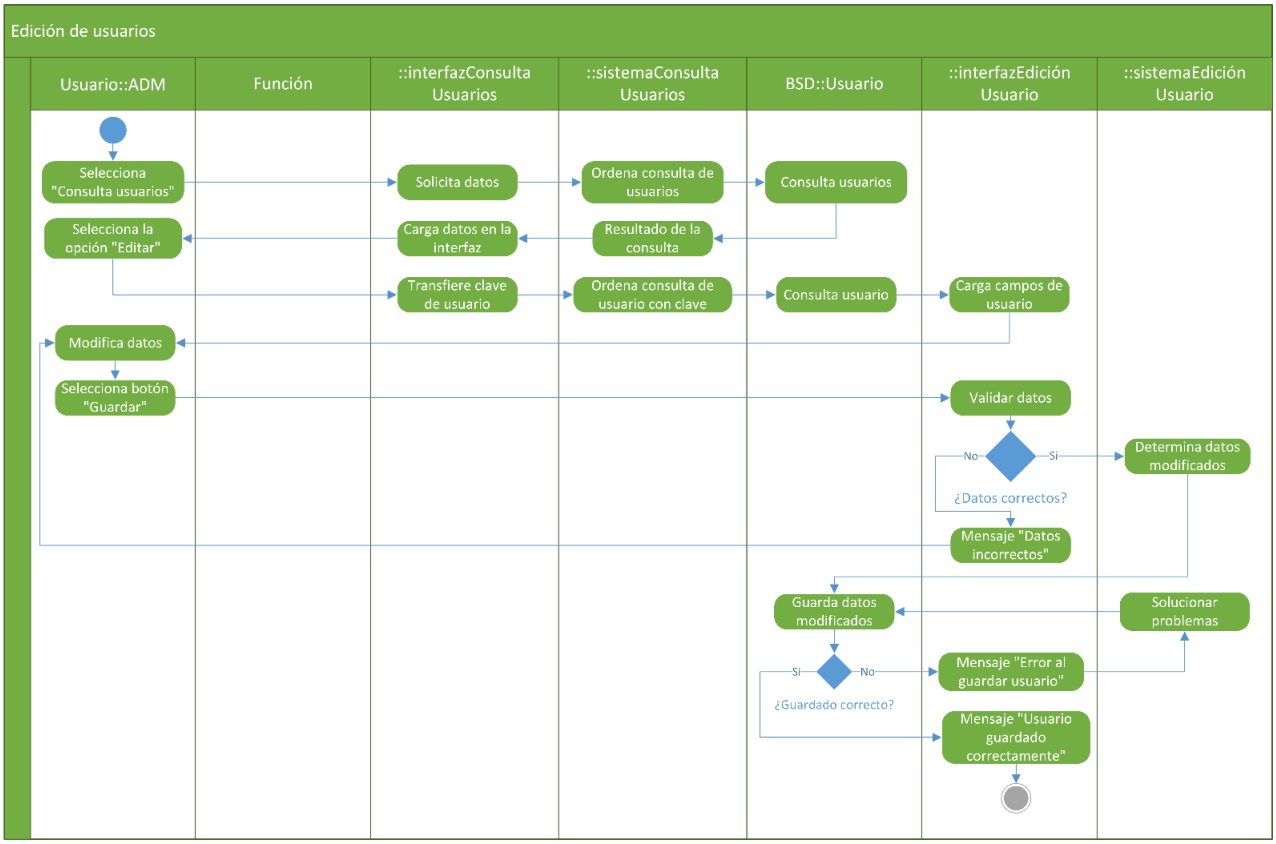

Ilustración 116: Edición de información de un usuario.
Fuente: Elaboración propia.

4.5. Modelo de configuración

En este modelo se especifica las características de hardware y software soportados, así también como las interfaces y la interacción de todos los componentes del sistema. (García Chi, 2013)

Para le representación de este modelo se utiliza el diagrama de despliegue. El diagrama de despliegue muestra la implementación física del sistema, incluye hardware, y las relaciones entre el hardware y el sistema. El diagrama de despliegue puede representar servidores, estaciones de trabajo, etc. Sirve para modelar la configuración del sistema. (García Chi, 2013)

4.5.1. Configuración general del sistema Ecu@Risk

La ilustración 117 representa la configuración general del sistema Ecu@Risk:

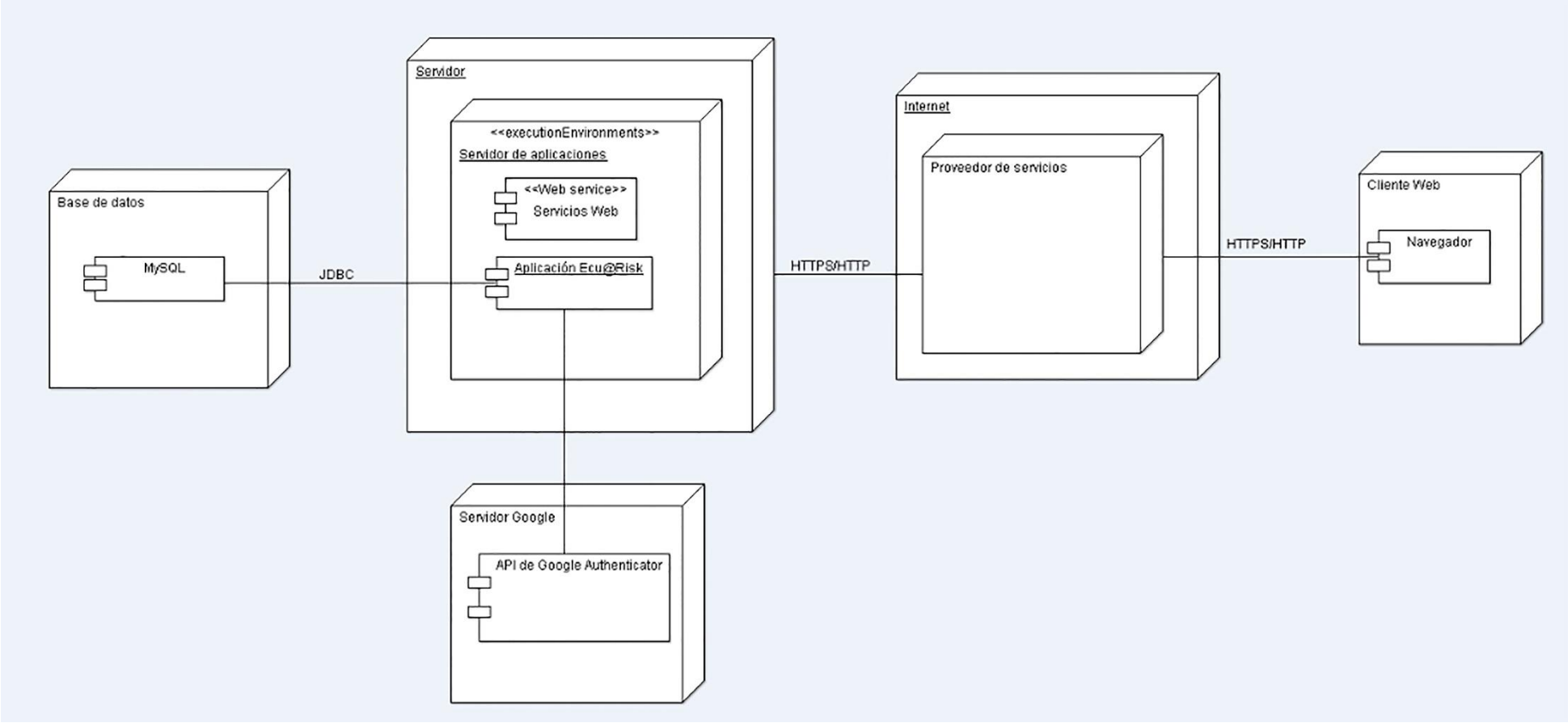

Ilustración 117: Configuración general del sistema Ecu@Risk.
Elaborados por: El autor.

4.6. Análisis relación navegación

García Chi (2013), indica que este análisis determina la estructura del sistema. El análisis relación navegación (ARN) proporciona una serie de pasos para identificar las relaciones entre los elementos del software, a continuación, se desarrollará cada uno de ellos.

4.6.1. Análisis de los participantes

En el sistema de gestión de seguridad de la información Ecu@Risk, existen tres tipos de usuarios, los usuarios Administradores (ADM), usuarios Coordinadores de Seguridad Designados (CSD) y finalmente los usuarios de Comité de Riesgo de Tecnología de Información (CRTI).

Administradores: Estos usuarios son los usuarios encargados del registro y modificación de los usuarios de todo el sistema Ecu@Risk, así mismo son los únicos autorizados para acceder al historial de acciones de los usuarios, para fines de auditoría y revisión.

Coordinadores de Seguridad Designados: Estos usuarios son expertos en gestión de seguridad de información, en el sistema Ecu@Risk, son los encargados de la identificación y gestión de activos de información. También se encargan de la gestión de los riesgos y la gestión de los planes de tratamiento para mitigar a dichos riesgos. Dentro de sus tareas en el sistema es la gestión de incidentes que hayan ocurrido en el negocio.

Comité de Riesgo de Tecnología de Información: Estos usuarios pertenecen a unidades estratégicas del negocio, es decir analizan los datos provenientes del sistema y toman decisiones para el negocio; son los encargados de gestionar los procesos de negocio y además pueden solicitar reportes de cuadro de mando integrado, así como de indicadores claves de negocio.

4.6.2. Análisis de los elementos

Para el análisis de los elementos del sistema Ecu@Risk se identificará los objetos de contenido y los elementos funcionales del sistema y se lo dividirá en diferentes categorías:

Categoría gestión de activos de información: en esta categoría se tienen a las clases: activo, baja o alta de activo, categoría de activo y clasificación de activo. La clase activo presenta los elementos funcionales de: registro de activo, consulta de activo, modificación de registro de activo, cambio de estado de activo y valorización de activo de información. La clase de registro de baja o alta de activo presenta los elementos funcionales de: registro, consulta de registro y modificación de información de registro. La clase categoría de activos presenta los elementos

funcionales de: registro, consulta y modificación de información. La clase clasificación de activos tienen elementos funcionales de: registro, consulta y modificación de información.

Categoría gestión de riesgos: en esta categoría se tienen a las clases: amenaza, clasificación de amenaza, riegos, baja o alta de riesgo y riesgo absoluto. La clase amenaza presenta elementos funcionales de: registro de amenaza, consulta y modificación de información. La clase categoría de amenaza presenta elementos funcionales de: registro, consulta y modificación de información. La clase riesgos presenta los elementos funcionales de: registro de riesgo, consulta de riesgo, modificación de información de registro de riesgo, cambio de estado de riesgo y valorización de riesgo. La clase registro de baja o alta de riesgo presenta los elementos funcionales: registro, consulta de registro y modificación de información de registro. La clase riesgo absoluto presenta los elementos funcionales de: cálculo de riesgo de disponibilidad, cálculo de riesgo de integridad, cálculo de riego de confidencialidad, cálculo de riesgo acumulado y consulta de riesgos.

Categoría gestión de tratamientos: en esta categoría se tienen a las clases: tratamiento, baja o alta de tratamiento, tipo de tratamiento, objetivo de tratamiento, actividades del plan de tratamiento y riesgo residual. La clase de tratamiento presenta los elementos funcionales de: registro de tratamiento, consulta de tratamiento, modificación de información de tratamiento, cambiar estado de un tratamiento y finalmente la medición del tratamiento. La clase registro de alta o baja de tratamiento tiene los siguientes elementos funcionales de: registro, consulta de registro y modificación de información del registro. La clase tipo de tratamiento presenta los elementos funcionales de: registro, consulta y modificación de información. La clase objetivo de tratamiento tiene los elementos funcionales de: registro, consulta y modificación de información. La clase actividades de tratamiento presenta los elementos funcionales de: registro, consulta y modificación de información. La clase riesgo residual presenta los elementos funcionales de: cálculo de riesgo de disponibilidad, cálculo de riesgo de integridad, cálculo de riesgo de confidencialidad, cálculo de riesgo de riesgo residual, consulta de riesgos.

Categoría de gestión de incidentes: en esta categoría se tiene la clase de incidentes; la clase incidentes presenta los elementos funcionales de: registro de incidentes, consulta de incidentes, modificación de información de incidentes.

Categoría de gestión procesos de negocio: en esta categoría se tienes las clases: procesos de negocio, registro de baja o alta de procesos de negocio, incidentes de procesos de negocio y estado de incidente. La clase incidentes presenta los elementos funcionales de: registro de

procesos de negocio, consulta y modificación de información de procesos de negocio. La clase de registro de baja o alta de procesos de negocio presenta los elementos funcionales de: registro, consulta de registros y modificación de información de registro. La clase incidentes de procesos de negocio tiene elementos funcionales de: registro, consulta y modificación de información. La clase estado de incidente presenta los elementos funcionales de registro, consulta y modificación de información.

Categoría de gestión de usuarios: en esta categoría se tiene las clases de: usuario, grupo y módulo. La clase usuario tiene los elementos funcionales de: registro de usuario, consulta de usuario, modificación de información de usuario y cambio de estado de usuario. La clase grupo tiene los elementos funcionales de: registro, consulta, modificación de información y eliminación. La clase módulo presenta los elementos funcionales de: registro, consulta, modificación de información y eliminación.

Categoría de parámetros: en esta categoría se tienen las clases de: parámetros y valores; la clase parámetros presenta los elementos funcionales de registro, consulta, modificación y eliminación. La clase valores tiene los elementos funcionales de: registro, consulta, modificación de información y eliminación.

4.6.3. Análisis de relaciones

A continuación, se analizarán las relaciones entre los elementos del sistema Ecu@Risk, Para ello, se lo dividirá en categorías.

Categoría de gestión de información

La categoría de gestión de riesgos de información tiene los siguientes elementos relacionados entre sí:

- La clase de “Activos” tiene los elementos:
    - “Registro de activo”, en donde se incluye el elemento de “Valorizar activo” (está oculto para el usuario, pero se lo utiliza para el registro de activo).
    - “Consulta de activos”.
    - “Consulta de detalles de activos” (es una derivación de la clase de consulta).
    - “Modificación de activos”
- La clase de “registro de baja o alta de activos” tiene los elementos:

- “Registro de baja o alta de activo”, en donde se incluye el elemento de “Cambiar estado de activo” (está oculto para el usuario, pero se lo utiliza para cambiar el estado del activo).
- “Consulta de baja o alta de activos”.
- “Modificación de baja o alta de activos”.

Todos estos elementos se alinean con el requisito del sistema de realizar un inventario de activos de información de la empresa.

La categoría de gestión de riesgos de información tiene los siguientes elementos relacionados entre sí:

- La clase de “Riesgos” tiene los elementos:
  - “Registro de riesgo”, en este elemento se incluye a la clase “Activos” ya que se eligen los activos de información a los que afecta dicho riesgo una condición previa es que los activos de información estén en estado activo, también se utiliza el elemento funcional “Valorizar riesgo” (está oculto para el usuario, pero se lo utiliza para el registro de riesgos).
  - “Consulta de riegos”.
  - “Consulta de detalles de riesgo” (es una derivación de la clase de consulta), “Modificación de riesgos”.
- La clase registro de baja o alta de riesgos tiene los siguientes elementos relacionados entre sí:
  - “Registro de baja o alta de riesgo”, en donde se incluye el elemento de “Cambiar estado de riesgo” (está oculto para el usuario, pero se lo utiliza para cambiar el estado del riesgo).
  - “Consulta de baja o alta de riesgos”.
  - “Modificación de baja o alta de riesgos”.

Todos estos elementos se alinean con el requisito del sistema de realizar un registro y seguimiento de riesgos que estén latentes en la empresa u organización.

La categoría de gestión de tratamientos tiene los siguientes elementos que se relacionan entre sí:

- La clase “Tratamiento” tiene los siguientes elementos:

- “Registro de tratamiento”, en este elemento se incluye a la clase “Tipo de tratamiento” y “Objetivo de tratamiento”, también está relacionado con la clase “Actividades de plan de tratamiento” ya que en el registro de planes de tratamiento también se hace uso de los elementos “Registro de actividades de planes de tratamiento”.
- “Consulta de tratamientos”.
- “Consulta de detalles de tratamiento” (es una derivación de la clase consulta) en este elemento se relaciona con el elemento “Consulta planes de tratamiento”.
- “Modificación de tratamientos” este elemento se relaciona directamente con el elemento “Modificación de planes de tratamiento”.
- “Medición de tratamientos”.

- La clase “Baja o alta de tratamiento” cuenta con los siguientes elementos:
  - “Registro de baja o alta de tratamiento”, en este elemento se incluye el elemento “Cambio de estado” (está oculto para el usuario, pero se lo utiliza para cambiar el estado del tratamiento), un tratamiento no podrá volver a estar activo si el riesgo al que mitigaba está siendo mitigado por otro plan de tratamiento.
  - “Consultar baja o alta de tratamiento”.
  - “Modificar baja o alta de tratamiento”.

Todos estos elementos se alinean con el requisito del sistema de realizar el registro de planes de tratamiento que ayuden a mitigar los riesgos que afecten a los activos de información.

La categoría gestión de incidentes tiene los siguientes elementos relacionados entre sí:

- La clase “Incidentes” tienen los elementos:
  - “Registro de incidentes”, este elemento se relaciona con las clases “Activos”, “Amenazas” y “Riesgos”.
  - “Consulta de incidentes”.
  - “Consulta detalle de incidentes” (es una derivación de la clase consulta).
  - “Modificación de incidentes”.

Todos estos elementos se alinean con el requisito del sistema de tener un registro de incidentes que ocurran dentro de la empresa u organización.

La categoría procesos de negocio tienen los siguientes elementos relacionados entre sí:

- La clase “Procesos de negocio” tiene los elementos:

- “Registro de procesos de negocio”, en este elemento se incluye a la clase “Activos” ya que un proceso de negocio cuenta con arios activos de información.
- “Consulta de procesos de negocio.
- “Consulta detalle de procesos de negocio” (es una derivación de la clase consulta).
- “Modificación de procesos de negocio”.

- La clase “Baja alta proceso de negocio” tiene los elementos:
  - “Registro de baja o alta de procesos de negocio” en este elemento se incluye “Cambio de estado” (está oculto para el usuario, pero se lo utiliza para cambiar el estado del proceso de negocio).
  - “Consulta de baja o alta de procesos de negocio”.
  - “Modificación de baja o alta de procesos de negocio”.
- La clase “Incidentes de proceso de negocio” tiene los elementos:
  - “Registro de incidente de proceso de negocio”, este elemento se relaciona con las clases “Estado de incidente”, “Incidentes” y “Procesos de negocio”.
  - “Consulta de incidente de proceso de negocio”.
  - “Consulta detalle de incidentes de proceso de negocio” (es una derivación del elemento de consulta).
  - “Modificación de incidente de procesos de negocio”.

Todos estos elementos se alinean con el requisito del sistema de tener un registro de los procesos de negocio tal como los incidentes que puedan ocurrir dentro de los mismos.

La categoría de usuarios tiene los siguientes elementos relacionados entre sí:

- La clase “Usuario” tiene los elementos:
  - “Registro de usuarios”, este elemento se asocia a la clase “Grupo”.
  - “Consulta de usuarios”.
  - “Consulta detalle de usuarios” (derivación del elemento de consulta).
  - “Modificación de usuarios”; la clase “Grupo” cuenta con los siguientes elementos “Registro de grupo” este elemento se asocia a la clase “Módulo”.
  - “Consulta de grupo”.
  - “Modificación de grupo”.
- La clase “Módulo” contiene los siguientes elementos:

- “Registro de módulo”.
- “Consulta de módulos”.
- “Modificación de módulos”.

Todos estos elementos se alinean con el requisito del sistema de manejar gestión de usuarios.

La categoría de gestión de parámetros tiene los siguientes elementos relacionados entre sí:

- La clase “Parámetros” cuenta con los elementos:
  - “Registro de parámetros”.
  - “Consulta de parámetros”.
  - “Modificación de parámetros”.
- La clase “Valores” cuenta con los elementos:
  - “Registro de valores”, este elemento está asociado a la clase “Parámetros”.
  - “Consulta de valores”.
  - “Modificación de parámetros”.

Todos estos elementos se alinean con el objetivo del sistema de valorizar activos de información, riesgos y planes de tratamiento.

4.6.4. Análisis de navegación

Cada categoría de usuario tiene su propia navegación, a continuación, se analizará la navegación de cada uno de ellos.

Los usuarios CSD tendrán acceso a la gestión de activos, gestión de riesgos, gestión de planes de tratamientos, gestión de incidentes y a los reportes. Los usuarios CRTI tendrán acceso a la gestión de procesos de negocio y reportes. Los usuarios ADM tendrán acceso a la gestión de usuarios.

Menú gestión de activos

Para registrar activos de información, el usuario debe acceder a la opción “Crear”; el sistema se redirige hacia un formulario de registro de activos, cuando se guarda la información el sistema indica si se guardó correctamente, si ocurre algún error el sistema notificará al usuario; luego se redirige a la pantalla de consulta de activos de información registrados.

Para consultar los activos de información del sistema, existen dos maneras: registrando un activo o seleccionado la opción “Listar”, en los dos casos el sistema lista todos los activos registrados en el sistema.

Para consultar los detalles de los activos, el usuario debe ingresar a la opción de “Listar”, luego acceder al ícono de “Detalles”; el sistema redirige hacia una ventana donde se presentan todos los detalles del activo registrado; para regresar a la ventana de consulta, el sistema presenta un botón de “Regresar”.

Para modificar la información de los activos, el usuario debe acceder al ícono de “Editar”, el cual está ubicado en la dentro ventana de “Listar” los activos de información; el sistema se redirige a una ventana donde se puede modificar la información del activo seleccionado, cuando se guarda la información el sistema indica que se guardó correctamente, si ocurre algún error el sistema notificará al usuario; el sistema se redirige hacia la ventana de consulta.

Para registrar un cambio de estado de un activo de información, el usuario debe acceder a la opción “Baja o alta”; el sistema se redirige hacia un formulario de registro, cuando se guarda la información, el sistema indica si se guardó correctamente, si ocurre algún error el sistema notificará al usuario; luego el sistema se redirige a la pantalla de consulta de los registros de baja o alta de activos que están notificados en el sistema.

Para consultar los registros de baja o alta de activos en el sistema, existen dos maneras: la primera es creando un registro de cambio de estado de activo o accediendo a la opción “Listar baja o alta”, en ambos casos el sistema lista todos los registros de cambio de estado de los activos de información.

Para modificar los registros de baja o alta de activos en el sistema el usuario debe acceder al ícono “Editar”, ubicado en la opción “Listar baja o alta”; el sistema se redirige a una ventana donde se puede modificar la información del registro seleccionado, cuando se guarda la información el sistema indica que se guardó correctamente, si ocurre algún error el sistema notificará al usuario.

Menú gestión de riesgos y tratamientos

Para e registro de riesgos, el usuario debe acceder a la opción “Crear riesgo”; el sistema se redirige hacia un formulario de registro de riesgo, cuando se requiera agregar a los activos afectados por el riesgo en el formulario, el sistema mostrará una ventana pequeña dentro de la pestaña principal, en la cual se eligen los activos; cuando se guarda la información el sistema indica si se guardó correctamente, si ocurre algún error el sistema notificará al usuario; el sistema se redirige a la pantalla de consulta de riesgos registrados.

Para consultar los riesgos, el usuario lo puede hacer de dos maneras: crear un riesgo o acceder a la opción “Listar riesgos”, en ambos casos el sistema lista a todos los riesgos en el sistema.

Para la consulta de detalles de un riesgo, el usuario debe estar ubicado en la ventana de “Listar riesgos”, y acceder al ícono de “Detalles”; el sistema se redirige hacia una ventana donde se muestran todos los detalles de los riesgos; para regresar a la ventana de consulta el sistema presenta el botón “Regresar”.

Para modificar la información de un riesgo, el usuario debe acceder al ícono “Editar” ubicado en la ventana de “Listar riesgos”; el sistema se redirige a una opción donde se puede modificar la información del riesgo seleccionado, cuando se guarda la información el sistema indica que se guardó correctamente, si ocurre algún error el sistema notificará al usuario.

Para registrar un cambio de estado de un riesgo, el usuario debe acceder a la opción “Baja o alta de riesgo”; el sistema se redirige hacia un formulario de registro, cuando se guarda la información, el sistema indica si se guardó correctamente, si ocurre algún error el sistema notificará al usuario; luego el sistema se redirige a la pantalla de consulta de los registros de baja o alta de riesgos que están notificados en el sistema.

Para consultar los registros de baja o alta de riesgos en el sistema, existen dos maneras: creando un registro de cambio de estado de riesgo o accediendo a la opción “Listar baja o alta de riesgos”, en ambos casos el sistema lista todos los registros de cambio de estado de los riesgos.

Para modificar los registros de baja o alta de riesgos en el sistema los usuarios deben acceder al ícono “Editar”, ubicado en la opción “Listar baja o alta de riesgos”; el sistema se redirige a una opción donde se puede modificar la información del registro seleccionado, cuando se guarda la información el sistema indica que se guardó correctamente, si ocurre algún error el sistema notificará al usuario; el sistema se redirige hacia la ventana de consulta.

Para consultar la relación entre los activos de información y los riesgos que los afectan, el usuario debe acceder a la opción “Relación activos y riesgos”; el sistema se redirige hacia una ventana en donde se listan los activos y cada uno de los riesgos que afectan a dichos activos de información.

Para registrar un plan de tratamiento el usuario debe acceder al ícono de “Definir plan de tratamiento” (cuando esté habilitado), dentro de la ventana “Relación activos y riesgos”, el

sistema se redirige hacia un formulario de registro un plan de tratamiento que mitigue el riesgo, cuando se guarde la información el sistema se redirige a la ventana de "Relación activos y riesgos" indicando que el plan ha sido guardado correctamente, si existe algún error al tratar de guardar el tratamiento, el sistema indicará al usuario.

Para indagar sobre los planes de tratamiento registrados en el sistema, el usuario debe acceder a la opción de "Listar planes de tratamiento", donde el sistema se redirige hacia una ventana en donde se listan todos los planes de tratamiento.

La consulta de un plan de tratamiento en específico, puede hacérselo de dos maneras: la primera es accediendo a la opción de "Relación activos riesgos", en donde, si ya se ha definido un plan de tratamiento para un riego, se podrá acceder al ícono "Detalles" (del plan de tratamiento); la segunda es acceder a la opción "Listar planes de tratamiento", en donde también podrá ver este ícono de "Detalles". Cuando el usuario acceda al ícono "Detalles"; el sistema se redirige hacia una ventana donde se muestra toda la información del plan de tratamiento; para regresar a la ventana de consulta el usuario tendrá un botón de "Regresar".

Para modificar la información de un plan de tratamiento, el usuario puede hacerlo de dos maneras: la primera es accediendo a la opción "Relación activos riesgos", en donde si ya se ha definido un tratamiento para un riesgo podrá acceder al ícono "Editar" (del plan de tratamiento); la segunda es acceder a la opción "Listar planes de tratamiento", en donde también podrá ver el ícono de "Editar". Cuando el usuario haga clic sobre el ícono "Editar", el sistema lo redirigirá hacia una ventana donde se muestra toda la información del plan de tratamiento y podrá editarla; cuando se guarde correctamente, el sistema se redirige hacia la venta anterior sea esta "Relación activos riesgos" o "Listar planes de tratamiento"; si el sistema detecta un error al tratar de guardar se le notificará al usuario.

Para imprimir los detalles de un plan de tratamiento, puede hacérselo de dos maneras: la primera es accediendo a la opción de "Relación activos riesgos" en donde si ya se ha definido un tratamiento para un riego podrá acceder al ícono "Imprimir" (del plan de tratamiento); la segunda es acceder a la opción "Listar planes de tratamiento", en donde también se podrá acceder ícono "Imprimir". Cuando se haga clic en el ícono "Imprimir"; el sistema se redirige hacia una ventana donde se muestra toda la información del plan de tratamiento y aparece un botón que dice "Imprimir", automáticamente se imprime el plan; el sistema regresa a la ventana de consulta, indicando el estado de la impresión.

Para realizar la medición de un plan de tratamiento, el usuario debe acceder a la opción "Listar planes de tratamiento", en donde aparece el ícono "Medir" (cuando la medición del plan esté disponible para realizarse); el sistema se redirige hacia una ventana en donde se registran los datos de la medición del plan de tratamiento; se guarda esta información y el sistema indica si se guardó correctamente y se redirige a la ventana de consulta, caso contrario si ocurrió algún error el sistema notifica al usuario.

Para registrar un cambio de estado de un tratamiento el usuario debe acceder a la opción "Baja o alta de tratamiento"; el sistema se redirige hacia un formulario de registro, cuando se guarda la información, el sistema indica si se guardó correctamente, si ocurre algún error el sistema notificará al usuario; posteriormente el sistema se dirige a la pantalla de consulta de los registros de baja o alta de los planes de tratamiento, los cuales están notificados en el sistema.

Para consultar los registros de baja o alta de tratamientos en el sistema, existen dos maneras: creando un registro de cambio de estado de tratamiento o accediendo a la opción "Listar baja o alta de tratamientos", en ambos casos el sistema lista todos los registros de cambio de estado de los tratamientos.

Para modificar los registros de baja o alta de tratamientos en el sistema, el usuario debe acceder al ícono "Editar", ubicado en la opción "Listar baja o alta de tratamientos"; el sistema se redirige a una opción donde se puede modificar la información del registro seleccionado; cuando se guarda la información el sistema indica que se guardó correctamente y se redirige a la ventana de consulta, si ocurre algún error el sistema notificará al usuario.

Para consultar la relación entre los activos de información, los riesgos que los afectan y los planes de tratamiento que los mitigan, el usuario debe acceder a la opción "Relación activos, riesgos y tratamientos"; el sistema se redirige hacia una ventana en donde se listan los activos cada uno de los riesgos que afectan a dichos activos de información y cada plan de tratamiento que mitiga a los riesgos.

Menú gestión de incidentes

Para el registro de un incidente, se lo debe hacer desde la opción "Crear"; el sistema se redirige hacia una ventana en donde se presenta el formulario de registro del incidente, cuando se requiera agregar a los activos afectados en incidente, el sistema presenta una pequeña ventana en la cual se pueden escoger los activos; cuando se guarde la información, el sistema indica si se guardó correctamente y se redirige hacia la lista de todos los incidentes registrados, caso contrario, si ocurre algún error el sistema notifica al usuario.

Para consultar los incidentes se lo puede hacer de dos maneras: registrando un nuevo incidente, o ingresando en la opción “Listar”, donde el sistema se redirige a una ventana en donde se listan todos los incidentes registrados.

La consulta de los detalles de un incidente se lo realiza ingresando en la opción “Listar”, posteriormente acceder al ícono de “Detalles”; el sistema se redirige a una ventana que muestra los detalles del incidente, para regresar a la ventana de consulta de los incidentes, está el botón de “Regresar”.

Para modificar la información de un incidente, el usuario debe acceder a la opción “Listar”, luego acceder al ícono de “Editar”; el sistema se redirige a una ventana donde muestra toda la información del registro seleccionado; cuando se guarde la información el sistema indica si se realizó correctamente y se redirige a la ventana de consulta, caso contrario, si ocurre algún error el sistema notifica al usuario.

Menú de gestión de procesos de negocio

El registro de un proceso de negocio se lo realiza ingresando en la opción “Crear proceso de negocio”; el sistema lo redirige hacia una ventana donde se presenta un registro de procesos de negocio, cuando se requiera agregar los activos de información a los procesos de negocio, el sistema muestra una pequeña ventana donde se eligen los activos a agregar; cuando se guarde la información el sistema indica si se realizó correctamente, caso contrario si ocurre algún error el sistema notifica al usuario; el sistema se redirige hacia la lista de todos los procesos de negocio registrados.

La consulta de los procesos de negocio se lo puede hacer de dos maneras: registrando un nuevo proceso de negocio, o ingresando en la opción “Listar procesos de negocio”, donde el sistema se redirige a una ventana en donde se listan todos los procesos de negocio registrados.

Para consultar los detalles de un proceso de negocio, el usuario debe acceder a la opción “Listar procesos de negocio”, seguidamente acceder al ícono de “Detalles”; el sistema se redirige a una ventana que muestra los detalles del proceso de negocio; para regresar a la ventana de consulta de procesos de negocio, está el botón de “Regresar”.

Para modificar la información de un proceso de negocio el usuario debe acceder a la opción “Listar procesos de negocio”, luego acceder al ícono de “Editar”, el sistema se redirige a una ventana donde muestra toda la información del registro seleccionado, cuando se guarde la

información el sistema indica si se realizó correctamente y se redirige a la ventana de consulta, caso contrario, si ocurre algún error el sistema notifica al usuario.

Para registrar un cambio de estado de un proceso de negocio el usuario debe acceder a la opción “Baja o alta de proceso de negocio”; el sistema redirige hacia un formulario de registro; cuando se guarda la información, el sistema indica si se guardó correctamente, si ocurre algún error el sistema notificará al usuario; posteriormente el sistema se redirige a la pantalla de consulta de los registros de baja o alta de tratamientos que están notificados en el sistema.

Para realizar la consulta de los registros de baja o alta de procesos de negocio en el sistema, existen dos opciones: creando un registro de cambio de estado de proceso de negocio o accediendo a la opción “Listar baja o alta de procesos de negocio”, en ambos casos el sistema lista todos los registros de cambio de estado de los procesos de negocio.

Para modificar los registros de baja o alta de procesos de negocio en el sistema, los usuarios deben acceder al ícono “Editar”, ubicado en la opción “Listar baja o alta de procesos de negocio”; el sistema se redirige a una opción donde se puede modificar la información del registro seleccionado; cuando se guarda la información el sistema indica que se guardó correctamente, si ocurre algún error el sistema notificará al usuario; el sistema se redirige a la ventana de consulta.

El registro de un seguimiento de proceso de negocio se lo realiza ingresando en la opción “Crear seguimiento de proceso de negocio”; el sistema se redirige hacia una ventana donde se presenta un registro para un seguimiento de procesos de negocio; cuando se requieran agregar incidentes al seguimiento, el sistema presenta una pequeña ventana, en la cual se puede elegir los incidentes; cuando se guarde la información el sistema indica si se realizó correctamente, caso contrario si ocurre algún error el sistema notifica al usuario; posteriormente el sistema se redirige hacia la lista de todos los seguimientos de procesos de negocio registrados.

Para consultar los seguimientos de procesos de negocio se lo puede hacer de dos maneras registrando un nuevo seguimiento de proceso de negocio, o ingresando en la opción “Listar seguimientos de procesos de negocio”, el sistema se redirige a una ventana en donde se listan todos los seguimientos de procesos de negocio registrados.

Para consultar los detalles de un seguimiento de proceso de negocio, el usuario debe acceder a la opción “Listar seguimientos de procesos de negocio”, luego hacer clic en el ícono de “Detalles”; el sistema se redirige a una ventana que muestra los detalles del seguimiento de proceso de negocio, para regresar a la ventana de consulta está el botón de “Regresar”.

Para modificar la información de un seguimiento de proceso de negocio, el usuario debe acceder a la opción “Listar seguimientos procesos de negocio”, luego ingresar en el ícono de “Editar”; el sistema se redirige a una ventana donde muestra toda la información del registro seleccionado, cuando se guarde la información el sistema indica si se realizó correctamente, caso contrario, si ocurre algún error el sistema notifica al usuario.

Menú de reportes

Para generar el reporte de cuadro de mando integrado (CMI), el usuario debe acceder a la opción “Reporte cuadro de mando integrado” y el sistema lo redirige hacia una ventana donde se presenta este reporte.

Para exportar este el reporte de cuadro de mando integrado (CMI), el usuario debe acceder a la opción “Reporte de cuando de mando integrado” y presionar el ícono de “Exportar” (debe elegir a qué formato desea exportar dicho reporte). Se exporta el reporte y se mantiene en la misma ventana de consulta notificando al usuario la acción realizada.

Para imprimir el reporte de cuadro de mando integrado (CMI), el usuario debe acceder a la opción “Reporte de cuando de mando integrado” y presionar el ícono de “Imprimir”. Se imprime el reporte y se mantiene en la misma ventana de consulta notificando al usuario la acción realizada.

Para generar el reporte de indicadores clave de desempeño de incidentes (KPI), el usuario debe acceder a la opción “Reporte de KPI de incidentes” y el sistema lo redirige hacia una ventana donde se presenta este reporte.

Para exportar este el reporte de indicadores clave de desempeño de incidentes, el usuario debe acceder a la opción “Reporte de KPI de incidentes” y presionar el ícono de “Exportar” (debe elegir a qué formato desea exportar dicho reporte). Se exporta el reporte y se mantiene en la misma ventana de consulta notificando al usuario la acción realizada.

Para imprimir este el reporte de indicadores clave de desempeño de incidentes, el usuario debe acceder a la opción “Reporte de KPI de incidentes” y presionar el ícono de “Imprimir”. Se imprime el reporte y se mantiene en la misma ventana de consulta notificando al usuario la acción realizada.

Para generar el reporte de indicadores clave de desempeño de planes de tratamiento (KPI), el usuario debe acceder a la opción “Reporte de KPI de planes de tratamiento” y el sistema lo redirige hacia una ventana donde se presenta este reporte.

Para exportar este el reporte de indicadores clave de desempeño de planes de tratamiento, el usuario debe acceder a la opción “Reporte de KPI de planes de tratamiento”,” y presionar el ícono de “Exportar” (debe elegir a qué formato desea exportar dicho reporte). Se exporta el reporte y se mantiene en la misma ventana de consulta notificando al usuario la acción realizada.

Para imprimir este el reporte de indicadores clave de desempeño de planes de tratamiento, el usuario debe acceder a la opción “Reporte de KPI de planes de tratamiento” y presionar el ícono de “Imprimir”. Se imprime el reporte y se mantiene en la misma ventana de consulta notificando al usuario la acción realizada.

Para generar el reporte de indicadores clave de desempeño de procesos de negocio (KPI), el usuario debe acceder a la opción “Reporte de KP I de procesos de negocio” y el sistema lo redirige hacia una ventana donde se presenta este reporte.

Para exportar este el reporte de indicadores clave de desempeño de procesos de negocio, el usuario debe acceder a la opción “Reporte de KPI de procesos de negocio”,” y presionar el ícono de “Exportar” (debe elegir a qué formato desea exportar dicho reporte). Se exporta el reporte y se mantiene en la misma ventana de consulta notificando al usuario la acción realizada.

Para imprimir este el reporte de indicadores clave de desempeño de procesos de negocio, el usuario debe acceder a la opción “Reporte de KPI de procesos de negocio” y presionar el ícono de “Imprimir”. Se imprime el reporte y se mantiene en la misma ventana de consulta notificando al usuario la acción realizada.

Menú de gestión de usuarios

Para registrar usuarios el usuario debe acceder a la opción “Crear”; el sistema se redirige hacia un formulario de registro de usuarios; cuando se guarda la información, el sistema indica si se guardó correctamente, si ocurre algún error el sistema notificará al usuario, luego se redirige a la pantalla de consulta de usuarios registrados.

Para consultar usuarios del sistema, existen dos maneras: registrando un usuario nuevo o seleccionado la opción “Listar”, en los dos casos el sistema lista todos los usuarios registrados en el sistema.

Para consultar los detalles de los usuarios, dentro de la opción de “Listar” los usuarios el sistema da la opción de “Detalles” con un ícono; el sistema se redirige hacia una venta donde se presentan todos los detalles del usuario registrado, para regresar a la ventana de consulta el sistema presenta un botón de “Regresar”.

Para modificar la información de los usuarios, el usuario debe acceder al ícono de “Editar” ubicado en la ventana de “Listar”, el sistema redirige a una opción donde se puede modificar la información del usuario seleccionado, cuando se guarda la información el sistema indica que se guardó correctamente, si ocurre algún error el sistema notificará al usuario.

4.7. Diseño de interfaces del sistema Ecu@Risk

A continuación, se presenta el diseño de las interfaces gráficas que representan al sistema Ecu@Risk.

La ilustración 118 representa la interfaz de inicio de sesión del sistema.

Ilustración 118: Interfaz de inicio de sesión.
Fuente: Elaboración propia.

La ilustración 119 representa la pantalla principal cuando el inicio de sesión sea de un usuario coordinador de seguridad designado (CSD).

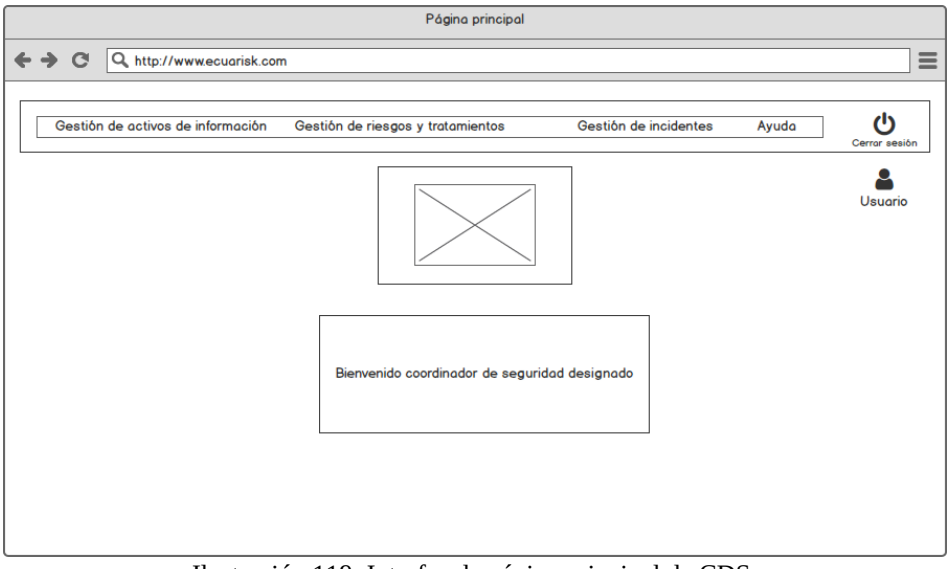

Ilustración 119: Interfaz de página principal de CDS.
Fuente: Elaboración propia.

La ilustración 120 representa los menús desplegados a los que el usuario coordinador de seguridad designado (CSD) tendrá acceso.

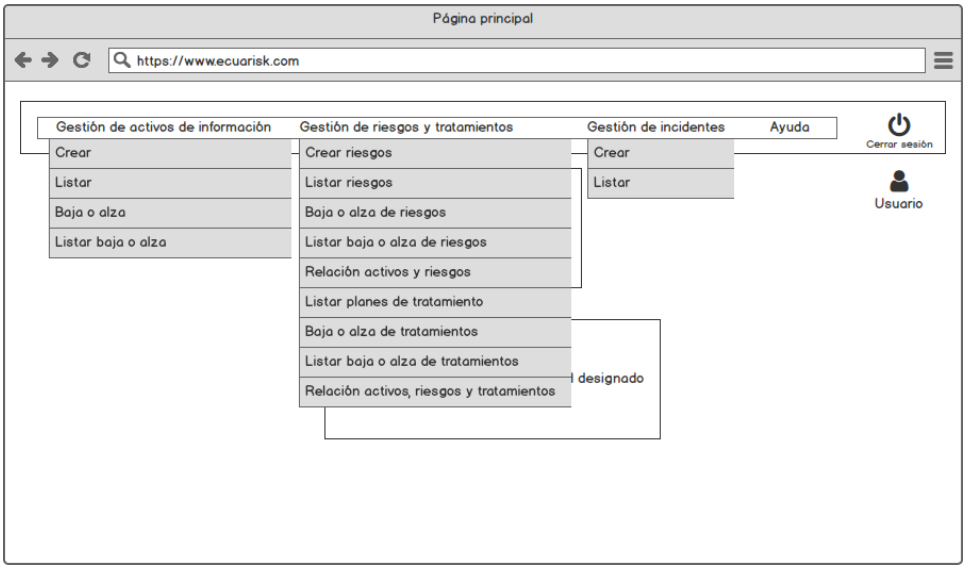

Ilustración 120: Interfaz de menús desplegados de CSD.
Fuente: Elaboración propia.

La ilustración 121 representa la pantalla principal cuando el inicio de sesión sea de un usuario de comité de riesgos de tecnologías de información (CRTI).

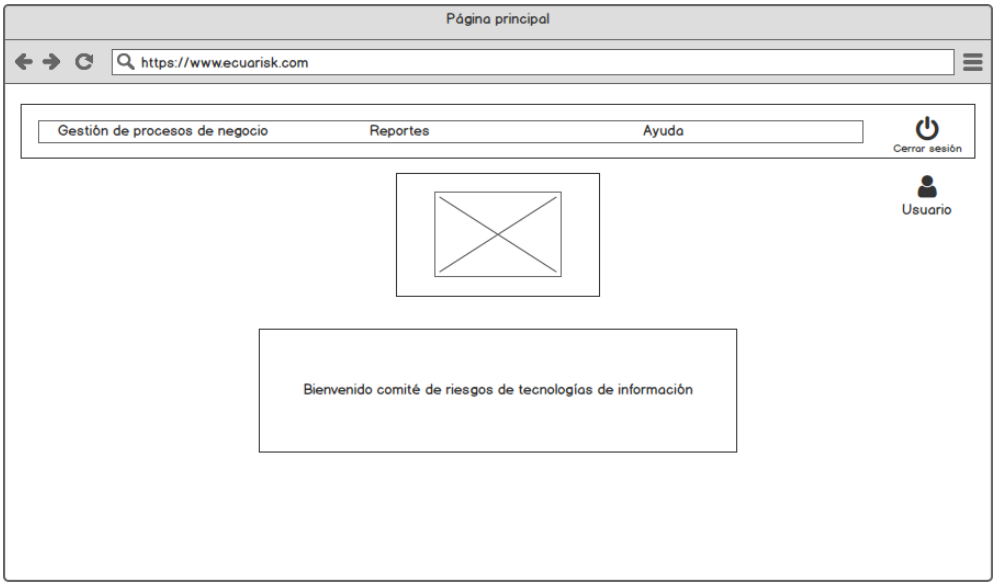

Ilustración 121: Página principal de CRTI.
Fuente: Elaboración propia.

La ilustración 122 representa los menús desplegados a los que el usuario de comité de riesgos de tecnologías de información (CRTI) tendrá acceso.

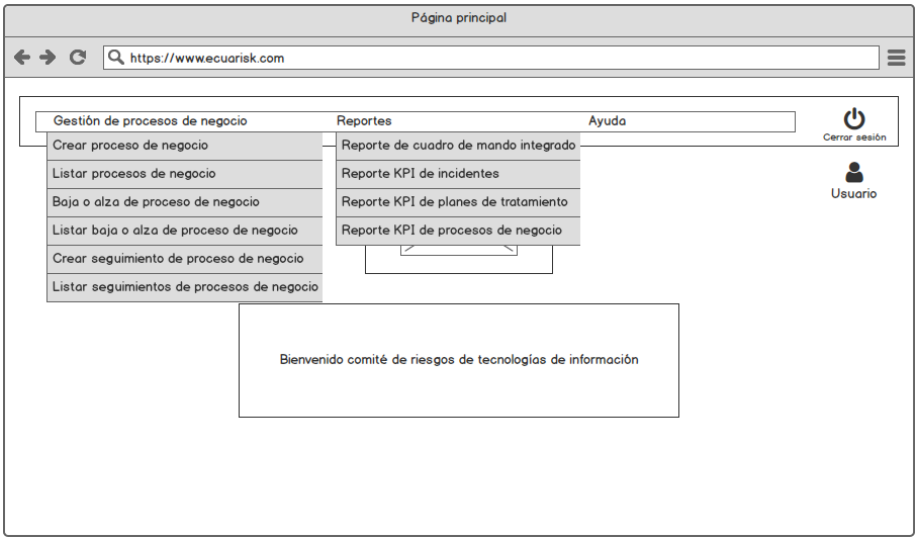

Ilustración 122: Interfaz de menús desplegados de CRTI.
Fuente: Elaboración propia.

La ilustración 123 representa la pantalla principal cuando el inicio de sesión sea de un usuario administrador (ADM).

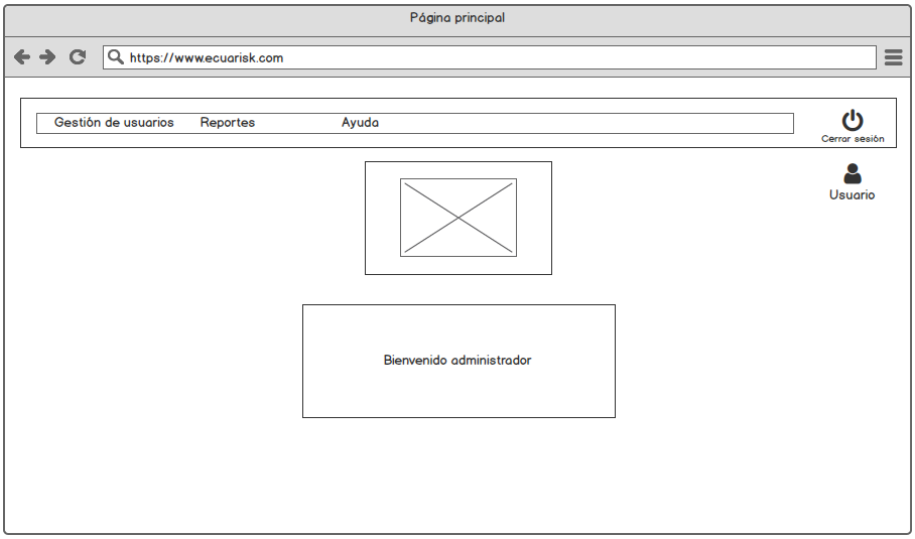

Ilustración 123: Interfaz pantalla principal de ADM.
Fuente: Elaboración propia.

La ilustración 124 representa los menús desplegados a los que el usuario administrador (ADM) tendrá acceso.

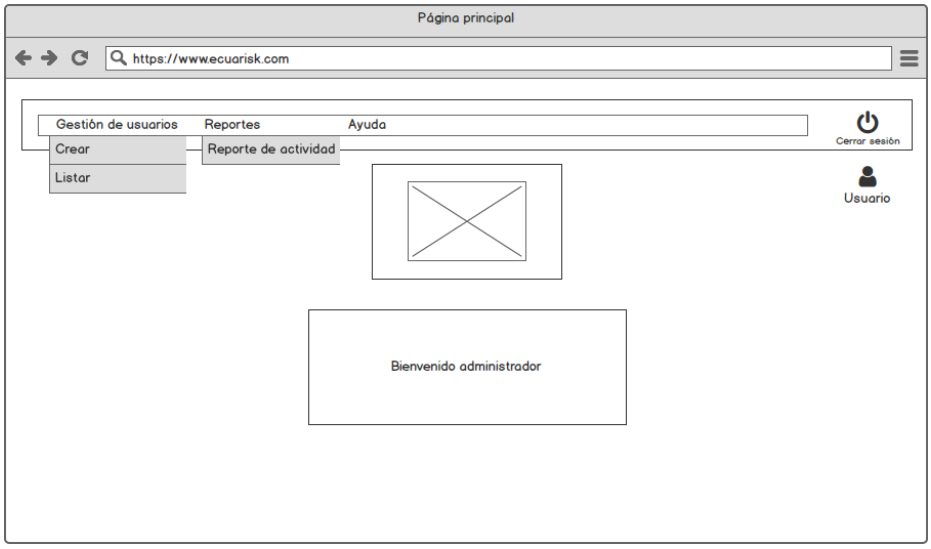

Ilustración 124: Interfaz menús desplegados de ADM.
Elaborado por. El autor.

La ilustración 125 representa la interfaz de registro de activos de información, también esta interfaz es utilizada para editar la información de un activo de información.

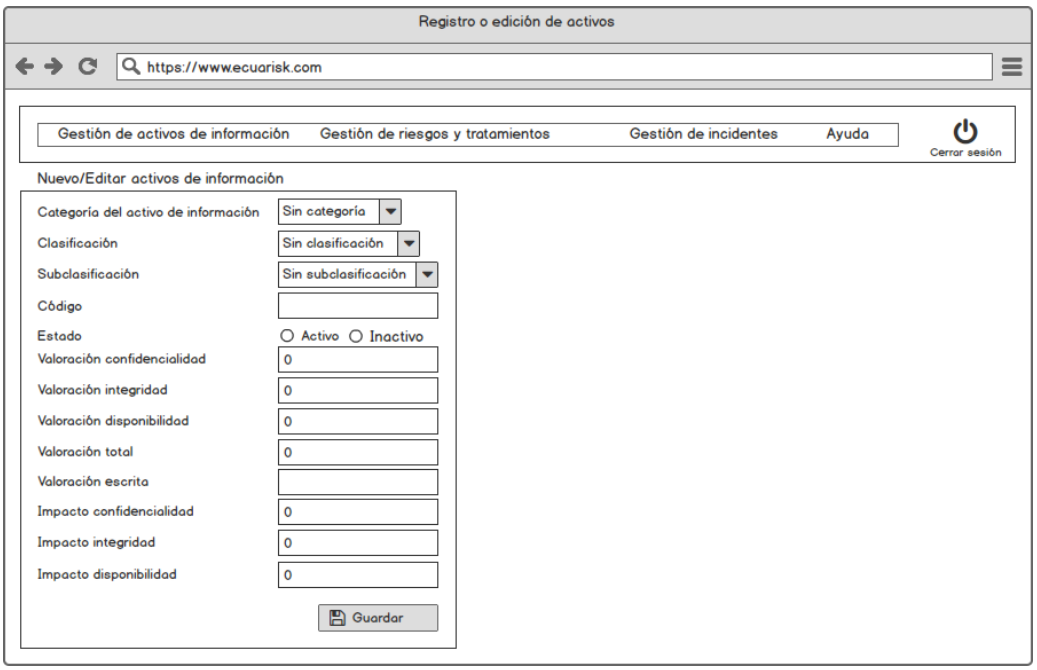

Ilustración 125: Interfaz de registro o edición de activos.
Fuente: Elaboración propia.

La ilustración 126 representa la interfaz gráfica de consulta de los activos de información registrados en el sistema, el ícono representa el acceso a los detalles del activo de información, el ícono representa el acceso a editar la información del activo.

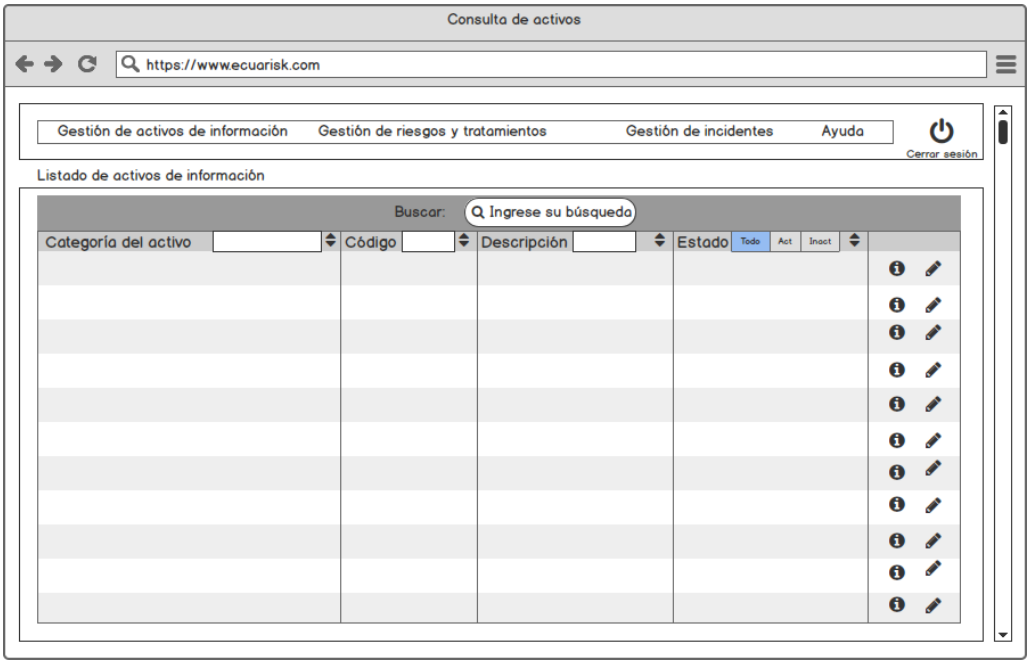

Ilustración 126: Interfaz de consulta de activos.
Fuente: Elaboración propia.

La ilustración 127 representa la interfaz de los detalles de un activo de información.

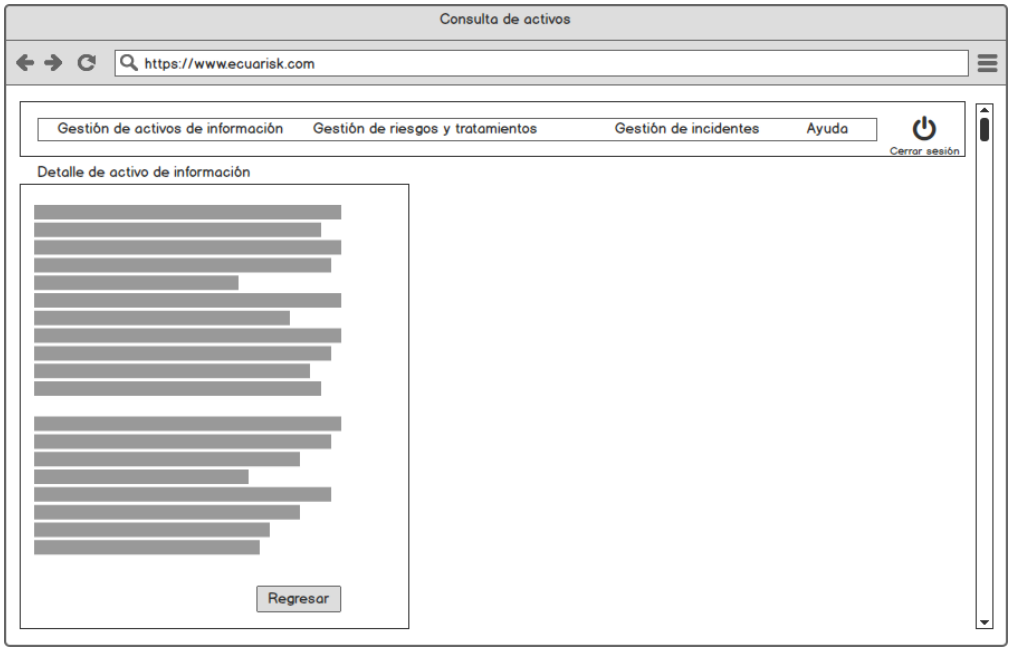

Ilustración 127: Interfaz de detalles de activo.
Fuente: Elaboración propia.

La ilustración 128 representa la interfaz de registro de una baja o alta de un activo de información, esta interfaz también es usada para la edición de información de un registro de alta o baja de un activo.

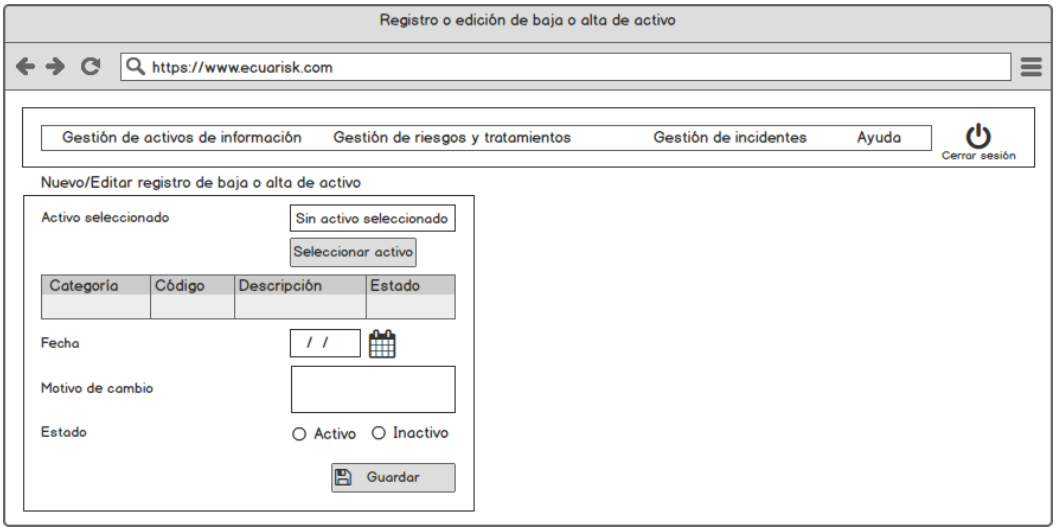

Ilustración 128: Interfaz de registro o edición de baja o alta de un activo.
Fuente: Elaboración propia.

La ilustración 129 representa la interfaz de registro o edición de baja o alta de activos de información, con la ventana emergente de selección de activos.

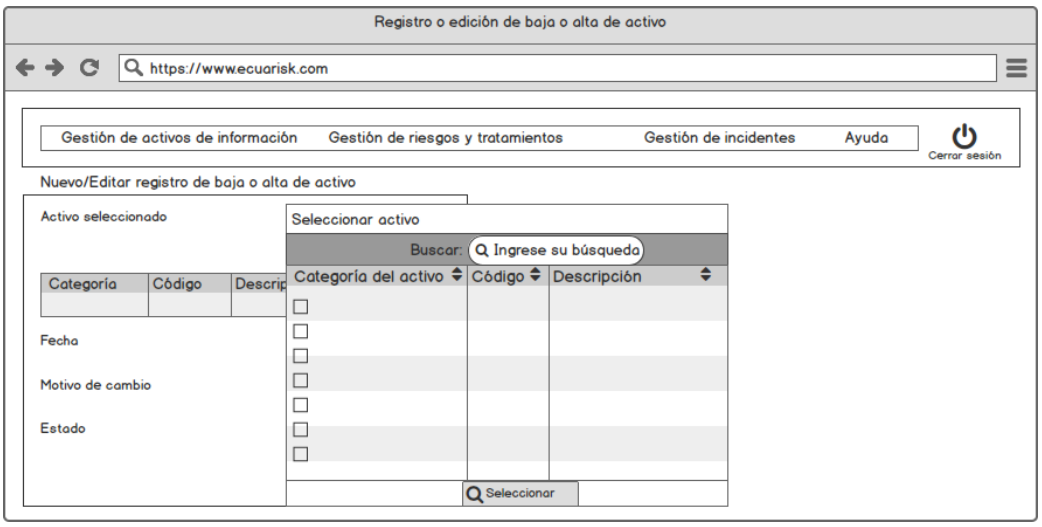

Ilustración 129: Interfaz de registro o edición de baja o alta de un activo con ventana emergente.

Fuente: Elaboración propia.

La ilustración 130 representa la interfaz de consulta de los registros de alta o baja de activos del sistema, el ícono ✎ representa el acceso a editar la información del registro.

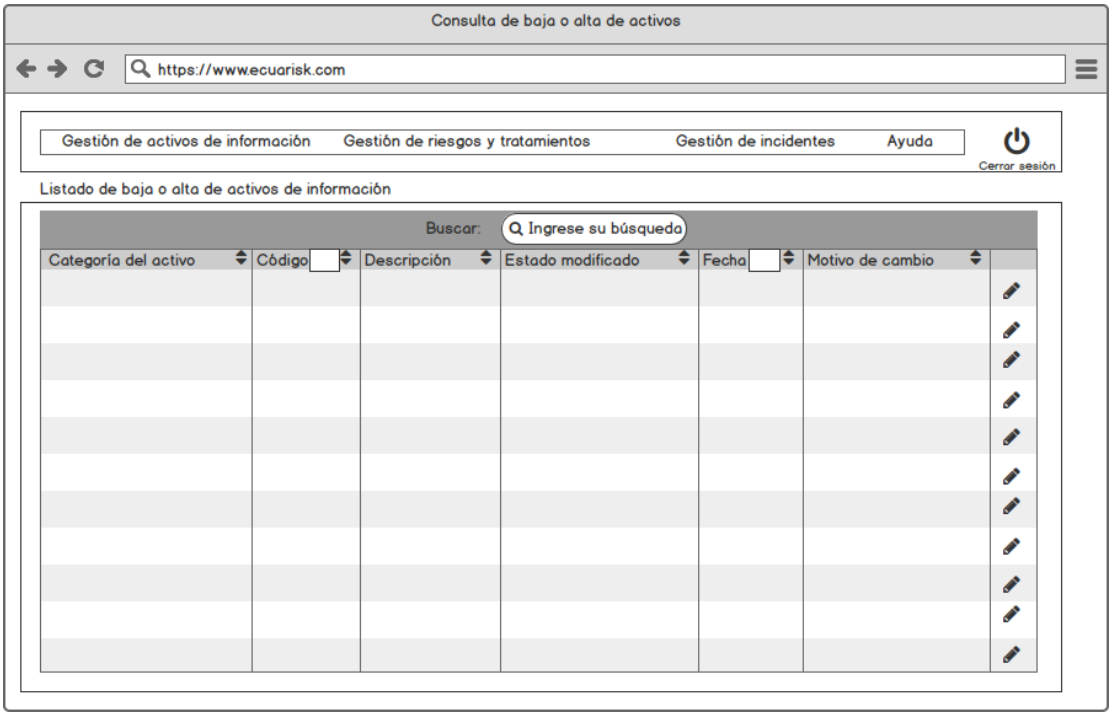

Ilustración 130: Interfaz de consulta de baja o alta de activos.
Fuente: Elaboración propia.

La ilustración 131 representa la interfaz gráfica del registro edición de información de un riesgo.

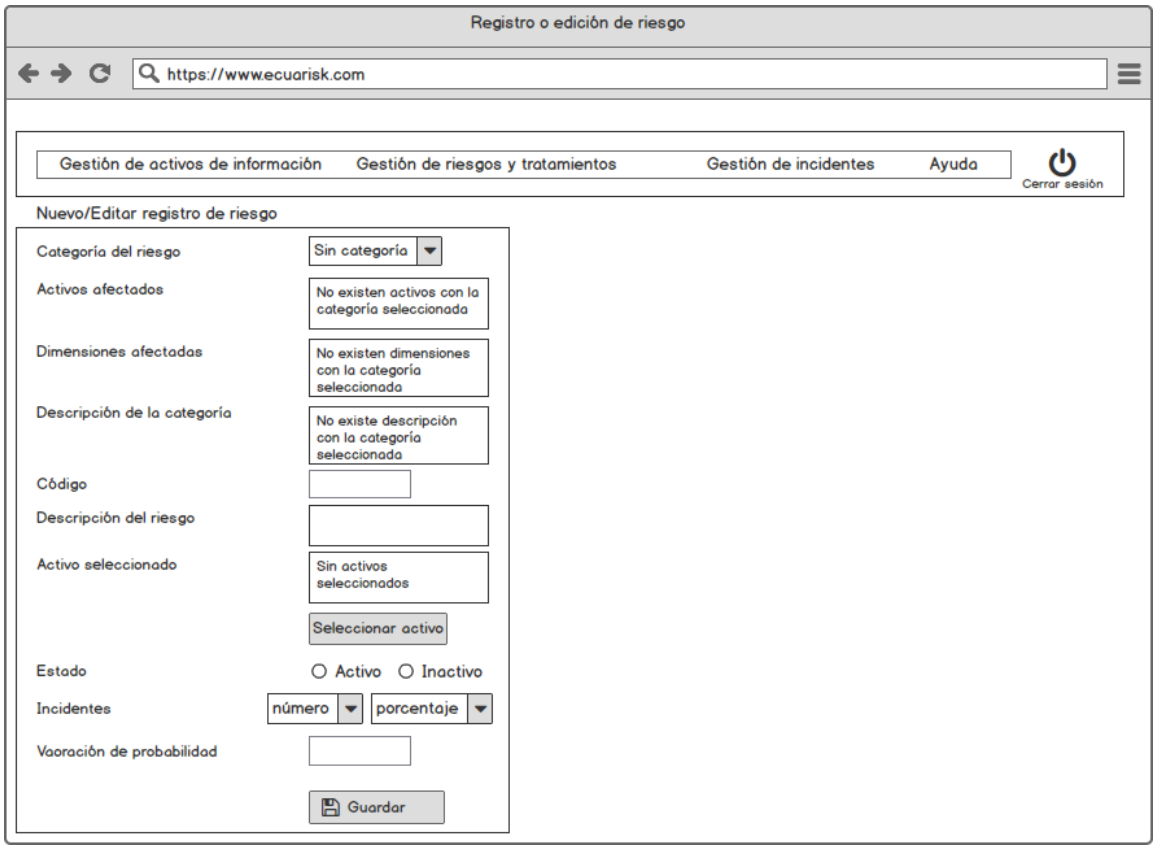

Ilustración 131: Interfaz de registro o edición de riesgo.
Fuente: Elaboración propia.

La ilustración 132 representa la interfaz gráfica del registro edición de información de un riesgo, con la ventana de selección de activos.

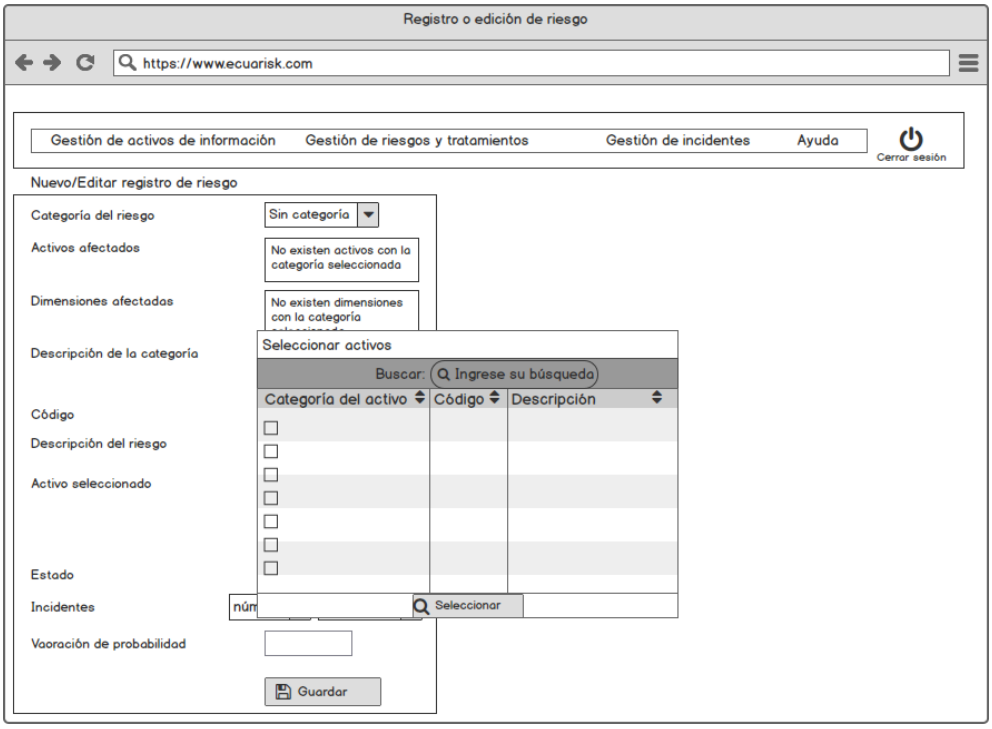

Ilustración 132: Interfaz de registro o edición de riesgo con ventana de elección de activos.
Fuente: Elaboración propia.

La ilustración 133 representa la interfaz gráfica de consulta de los riesgos registrados en el sistema, el ícono ℹ representa el acceso a los detalles del riesgo, el ícono ✎ representa el acceso a editar la información del riesgo.

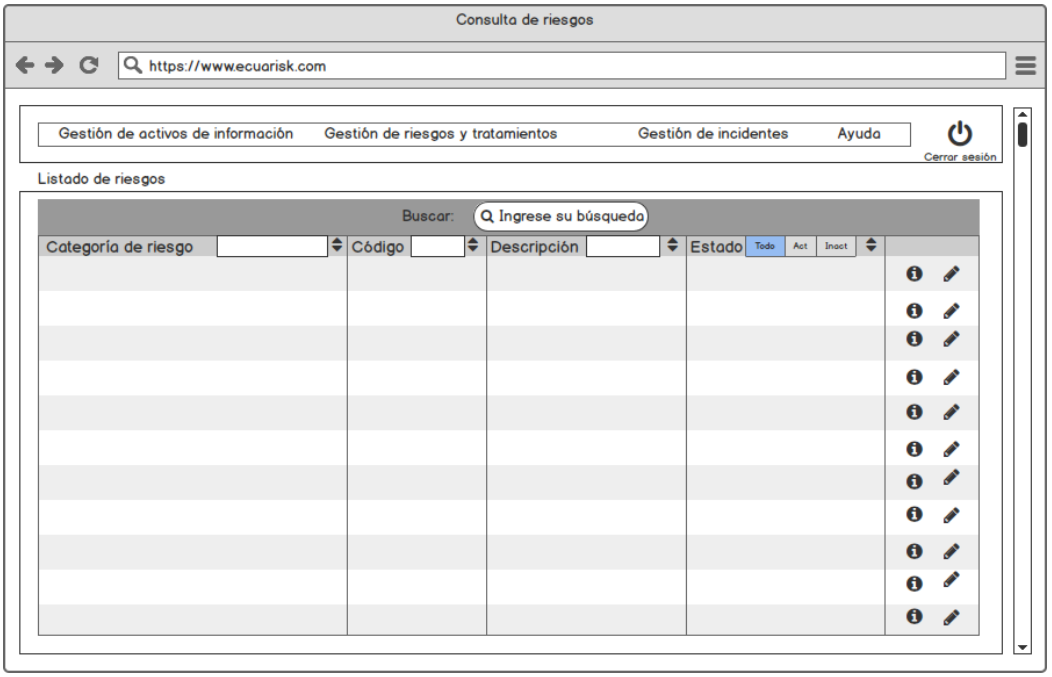

Ilustración 133: Interfaz de consulta de riesgos.
Fuente: Elaboración propia.

La ilustración 134 representa la consulta de los detalles de un riesgo.

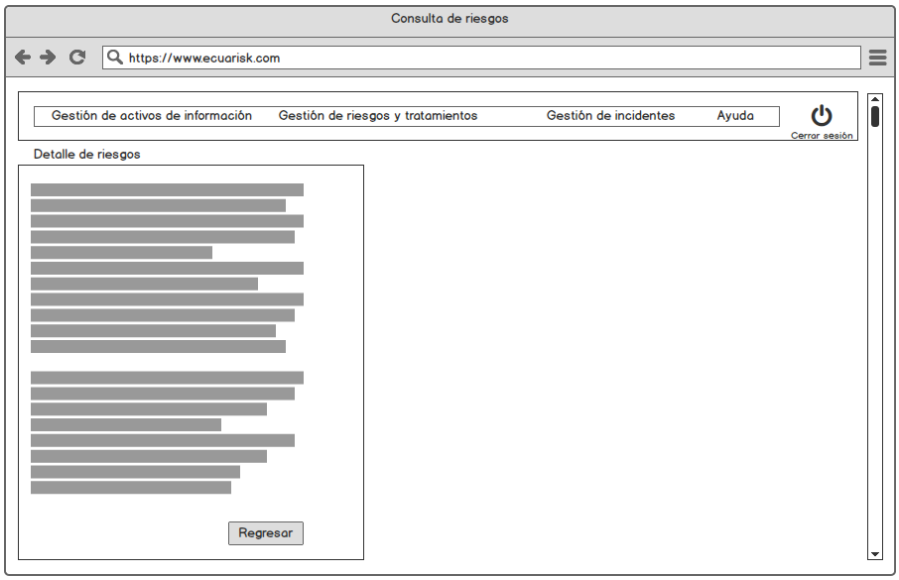

Ilustración 134: Interfaz de consulta de detalles de riesgo.
Fuente: Elaboración propia.

La ilustración 135 representa la relación entre los activos y cada uno de sus riesgos. Cuando un plan de tratamiento está definido para el riesgo aparecen los íconos: ℹ, ✎ y 🖶, los cuales representan el acceso a detalles de plan de tratamiento, editar la información del plan de tratamiento e imprimir el plan de tratamiento, respectivamente. Cuando el riesgo no tiene definido ningún plan de tratamiento el sistema muestra el ícono ✎, el cual representa definir un plan de tratamiento.

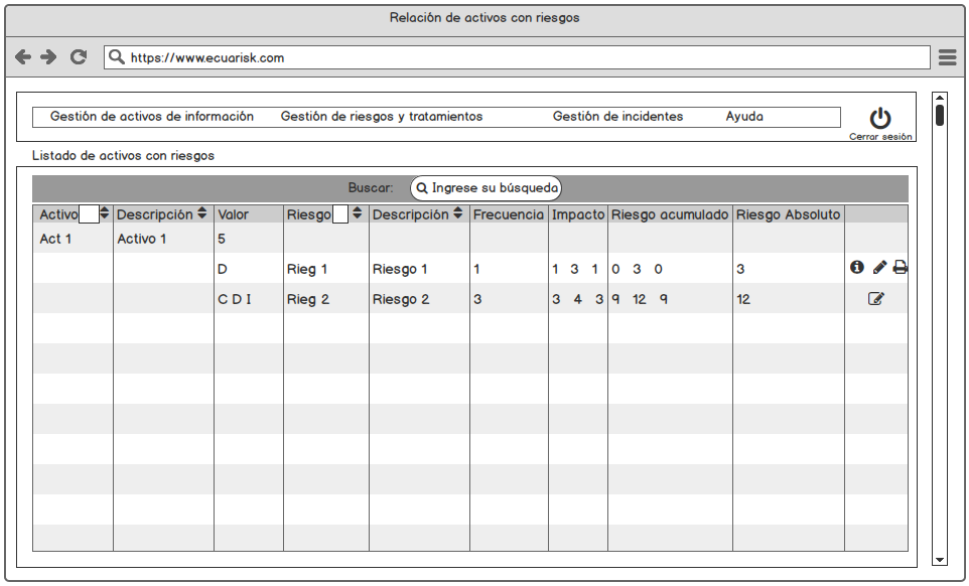

Ilustración 135: Interfaz de relación de activos y riesgos.
Fuente: Elaboración propia.

La ilustración 136 representa la interfaz gráfica de registro y edición de información de un plan de tratamiento.

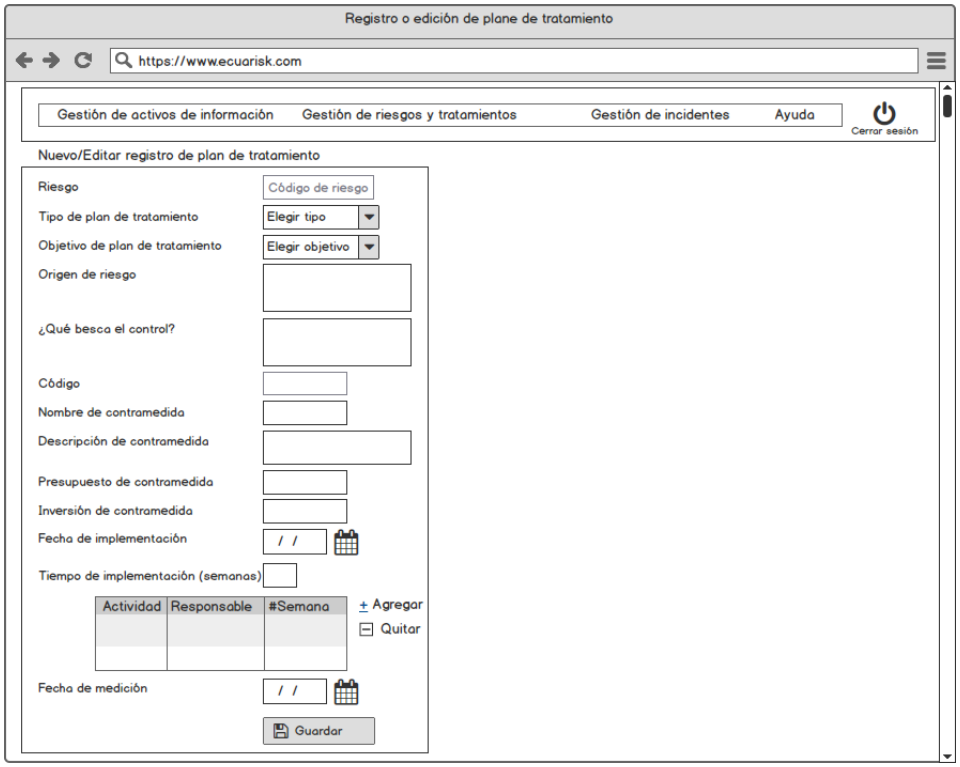

Ilustración 136: Interfaz de registro o edición de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 137 representa la interfaz gráfica de los planes de tratamiento registrados en el sistema. Cada plan de tratamiento cuenta con los siguientes íconos: ℹ, ✎ y 🖶, los cuales representan el acceso a detalles de plan de tratamiento, editar la información del plan de tratamiento e imprimir el plan de tratamiento, respectivamente. Adicionalmente cuando un plan de tratamiento esté listo para ser medido el sistema muestra el ícono 🕘, el cual representa el acceso a la medición de un plan de tratamiento.

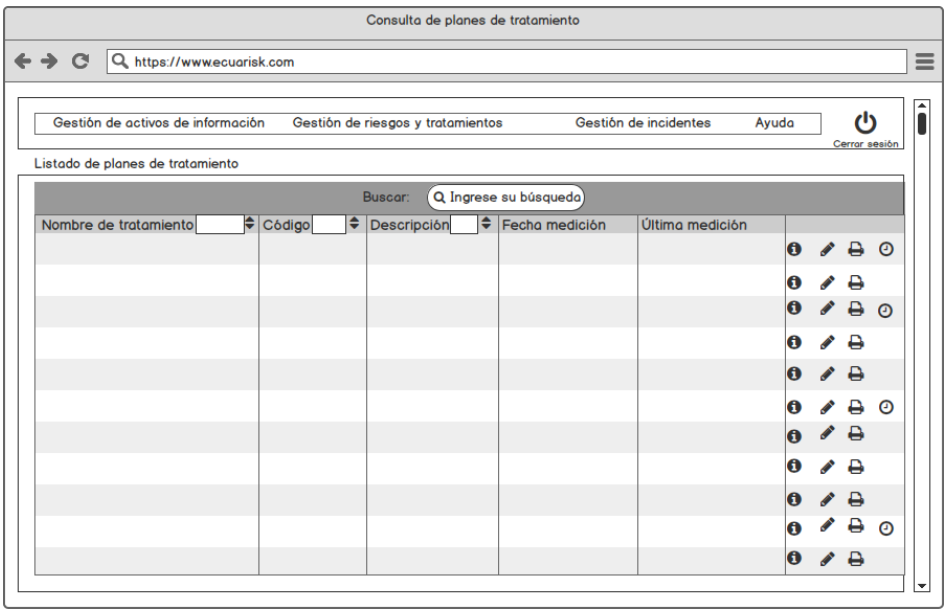

Ilustración 137: Interfaz de consulta de planes de tratamiento.
Fuente: Elaboración propia.

La ilustración 138 representa la interfaz gráfica de la consulta de los detalles de un plan de tratamiento.

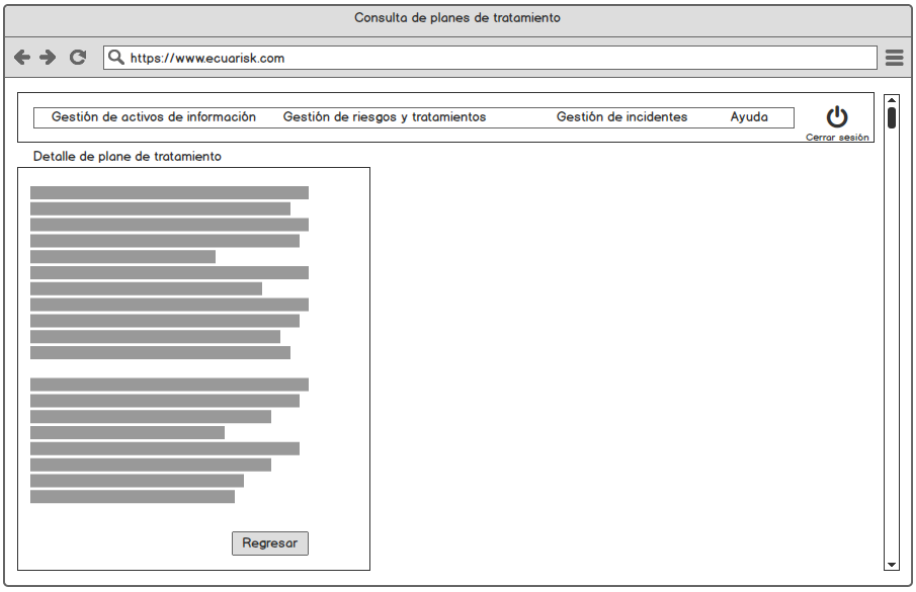

Ilustración 138:Interfaz de consulta de detalles de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 139 representa la interfaz gráfica de la medición de un plan de tratamiento.

Ilustración 139: Interfaz de medición de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 140 representa la interfaz gráfica de la relación entre activos, riesgos y planes de tratamiento

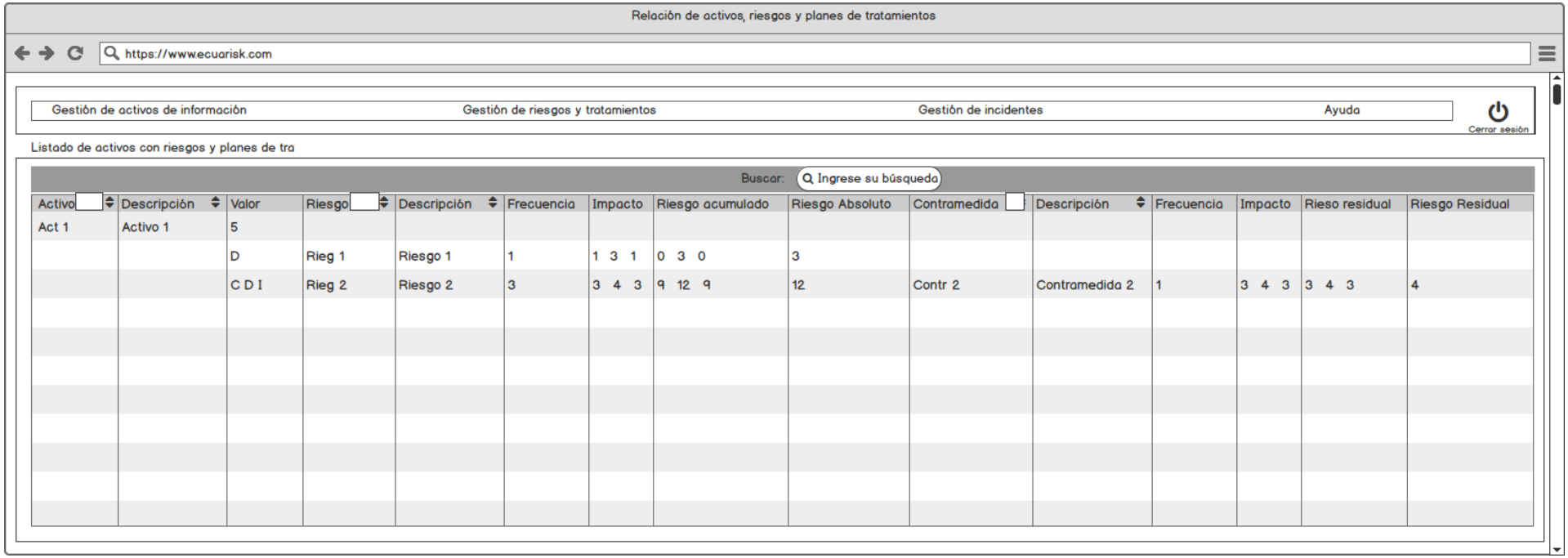

Ilustración 140: Interfaz de relación activos, riesgos y planes de tratamiento.
Fuente: Elaboración propia.

La ilustración 141 representa la interfaz de registro de una baja o alta de un riesgo, esta interfaz también es usada para la edición de información de un registro de alta o baja de un riesgo.

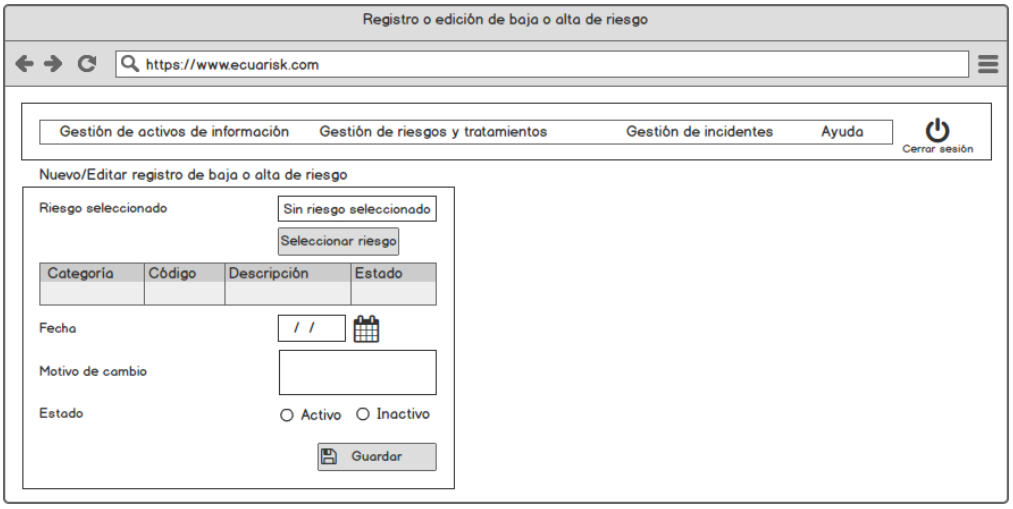

Ilustración 141: Interfaz de registro o edición de baja o alta de un riesgo.
Fuente: Elaboración propia.

La ilustración 142 representa la interfaz de registro o edición de baja o alta de riesgos, con la ventana emergente de selección de riesgo.

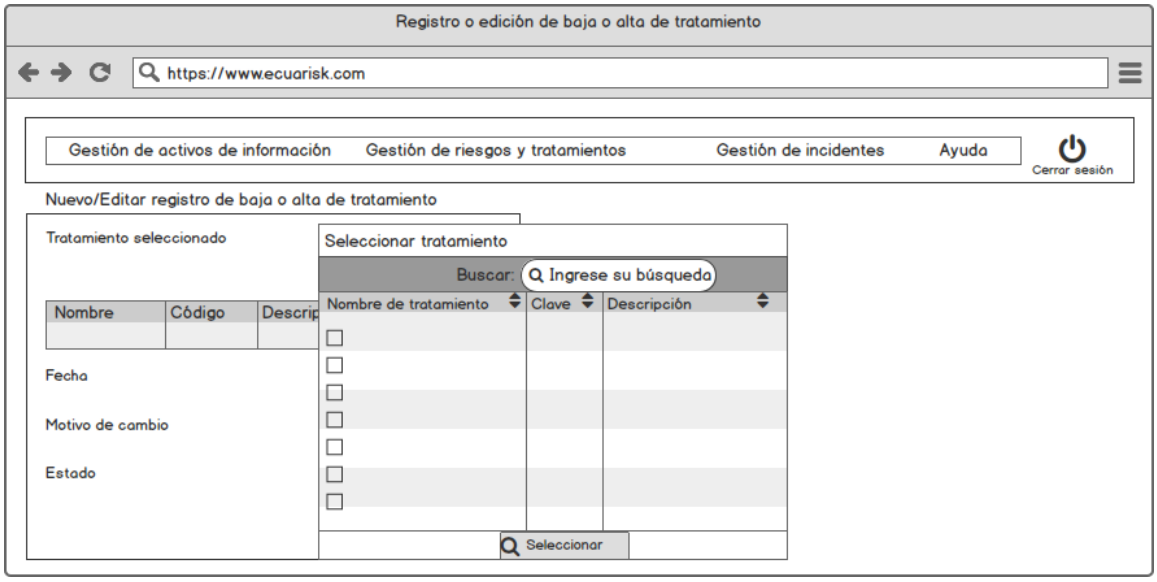

Ilustración 142: Interfaz de registro o edición de baja o alta de un riesgo con selección de riesgo.
Fuente: Elaboración propia.

La ilustración 143 representa la interfaz de consulta de los registros de alta o baja de riesgos del sistema, el ícono ✎ representa el acceso a editar la información del registro.

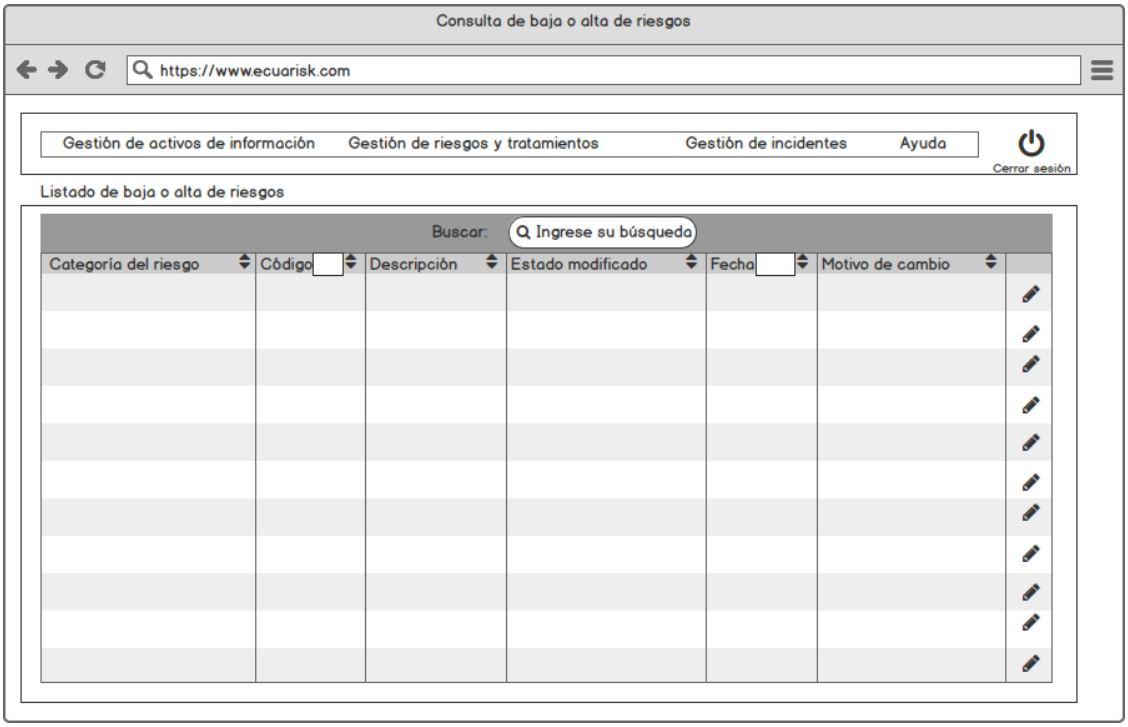

Ilustración 143: Interfaz de consulta de baja o alta de riesgos.
Fuente: Elaboración propia.

La ilustración 144 representa la interfaz de registro o edición de información de una baja o alta de un plan de tratamiento.

Ilustración 144: Registro o edición de baja o alta de plan de tratamiento.
Fuente: Elaboración propia.

La ilustración 145 representa la interfaz de registro o edición de baja o alta de tratamientos, con la ventana emergente de selección de tratamiento.

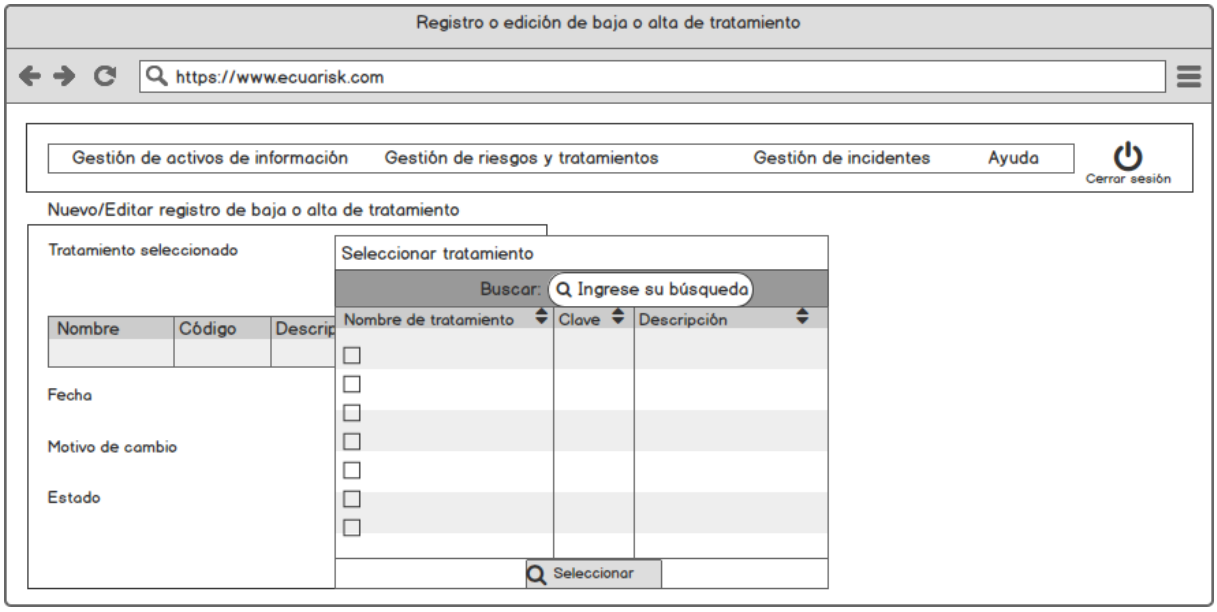

Ilustración 145: Interfaz de registro o edición de baja o alta de tratamientos con selección de tratamiento.
Fuente: Elaboración propia.

La ilustración 146 representa la interfaz de consulta de los registros de alta o baja de planes de tratamiento, el ícono ✎ representa el acceso a editar la información del registro.

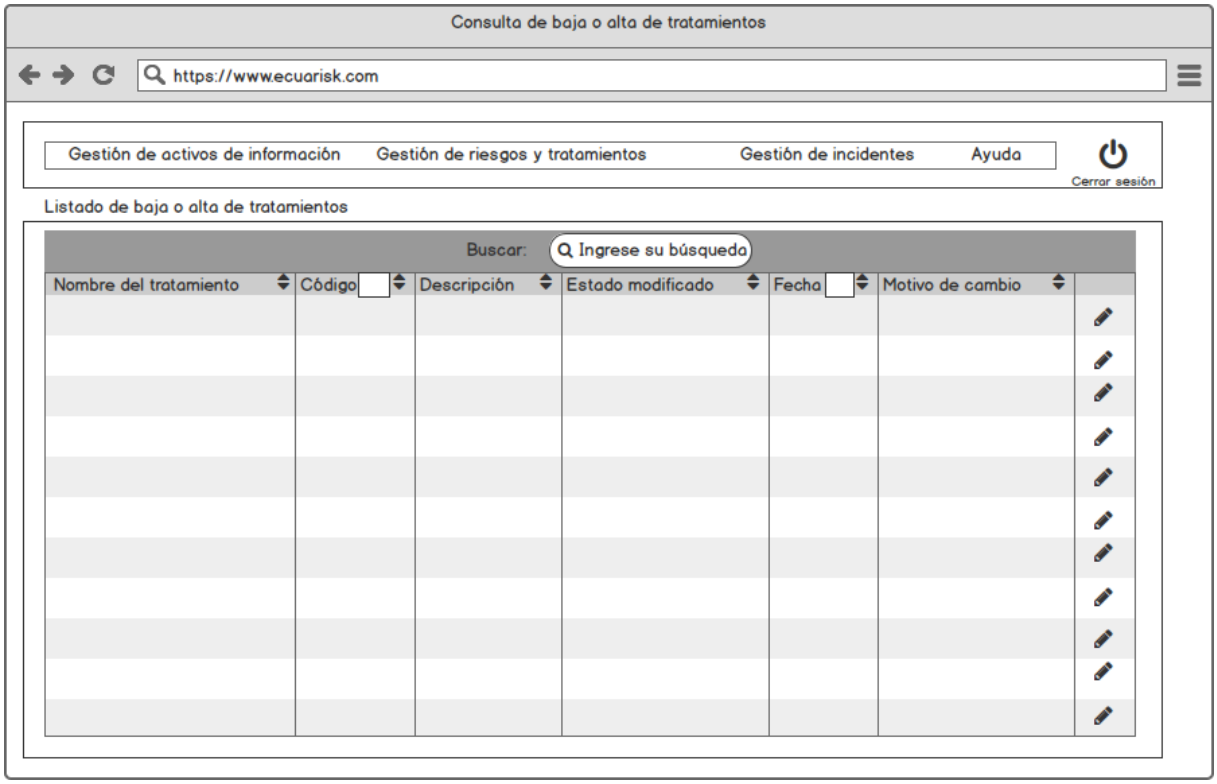

Ilustración 146: Consulta baja o alta de planes de tratamiento.
Fuente: Elaboración propia.

La ilustración 147 representa la interfaz gráfica del registro o edición de información de un incidente.

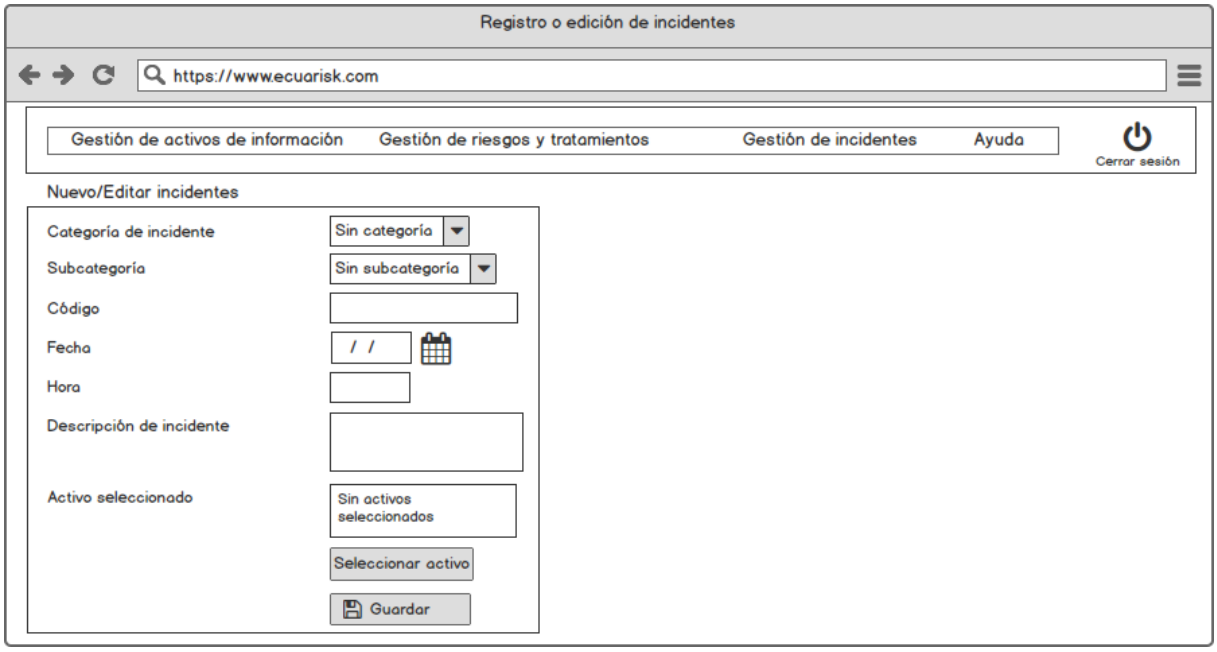

Ilustración 147: Interfaz de registro o edición de incidentes.
Fuente: Elaboración propia.

La ilustración 148 representa la interfaz gráfica del registro o edición de información de un incidente, con la ventana emergente de selección de activos.

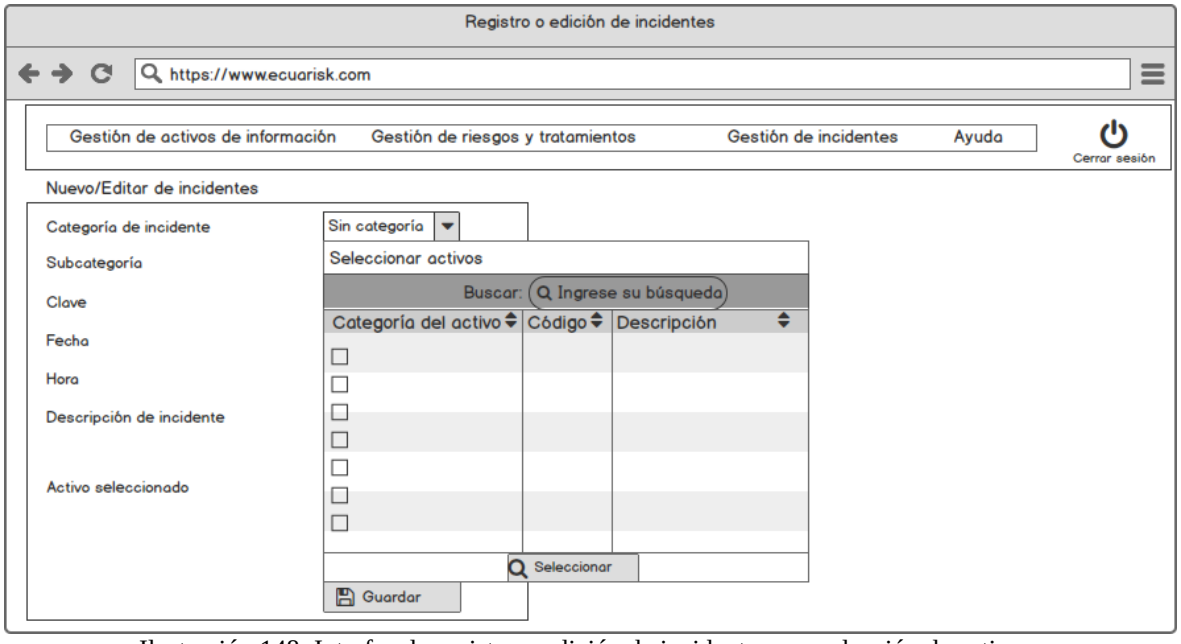

Ilustración 148: Interfaz de registro o edición de incidentes con selección de activos.
Fuente: Elaboración propia.

La ilustración 149 representa la interfaz gráfica de la consulta de los incidentes registrados en el sistema, el ícono ℹ representa el acceso a los detalles del incidente, el ícono ✎ representa el acceso a editar la información del incidente.

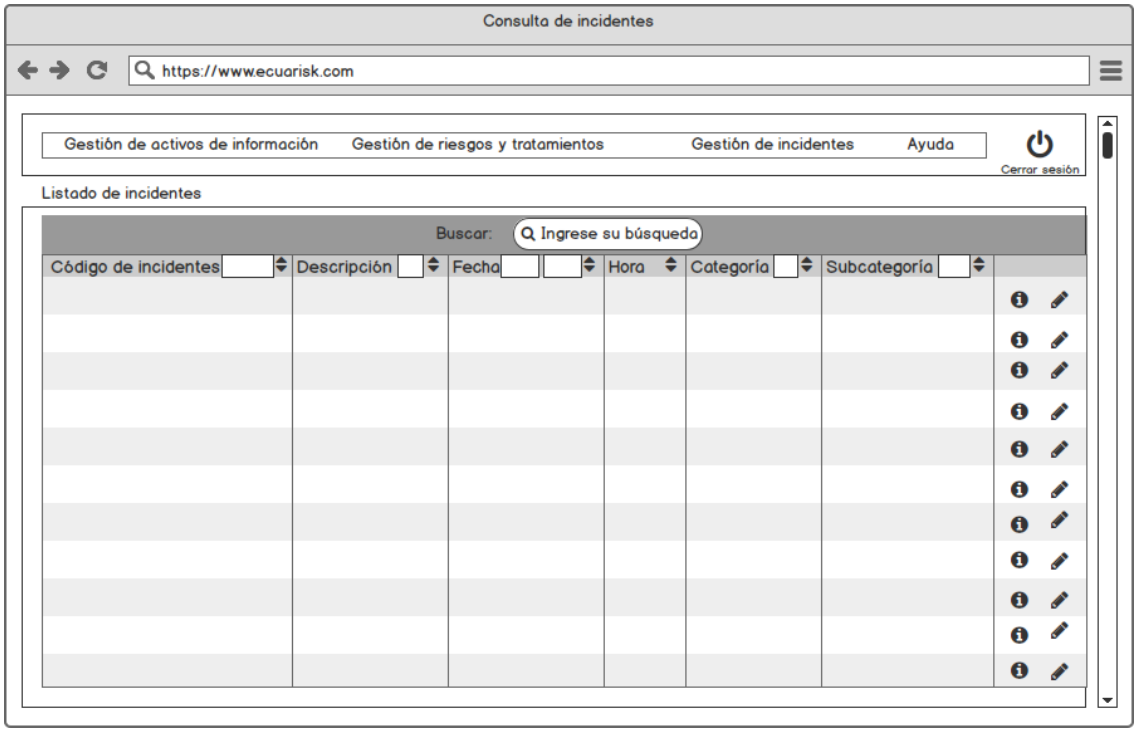

Ilustración 149: Interfaz de consulta de incidentes.
Fuente: Elaboración propia.

La ilustración 150 representa la interfaz gráfica de consulta de detalles de un incidente.

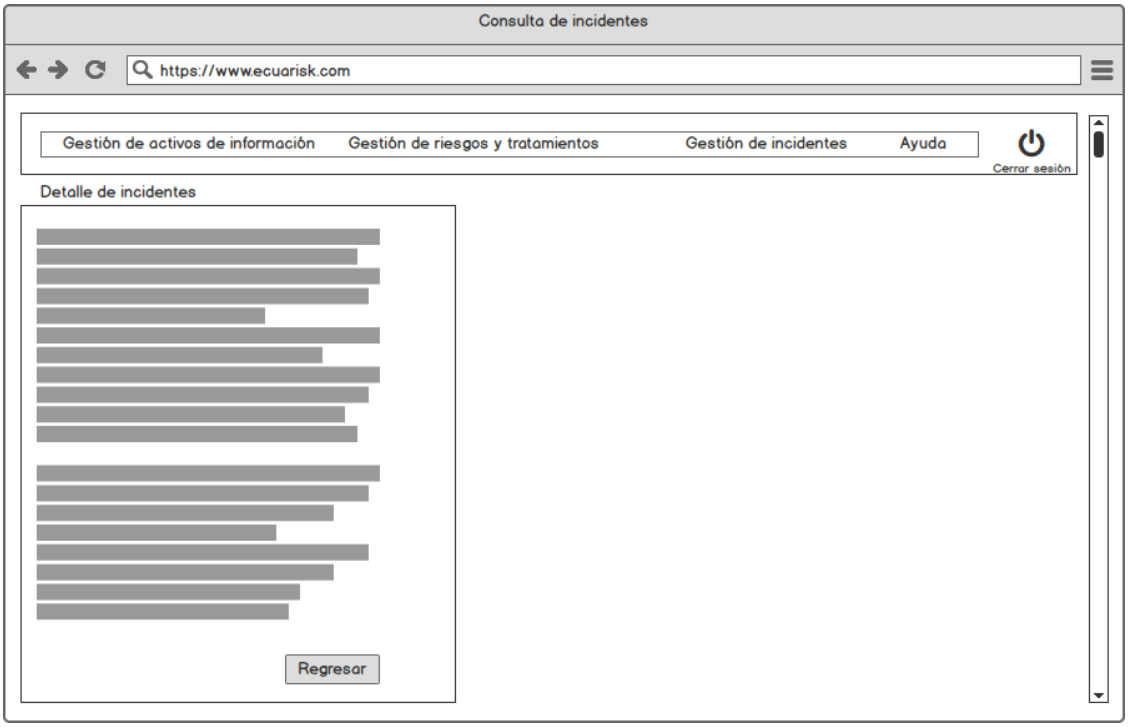

Ilustración 150: Interfaz de consulta de detalles de incidente.
Fuente: Elaboración propia.

La ilustración 151 representa el registro o edición de información de un proceso de negocio.

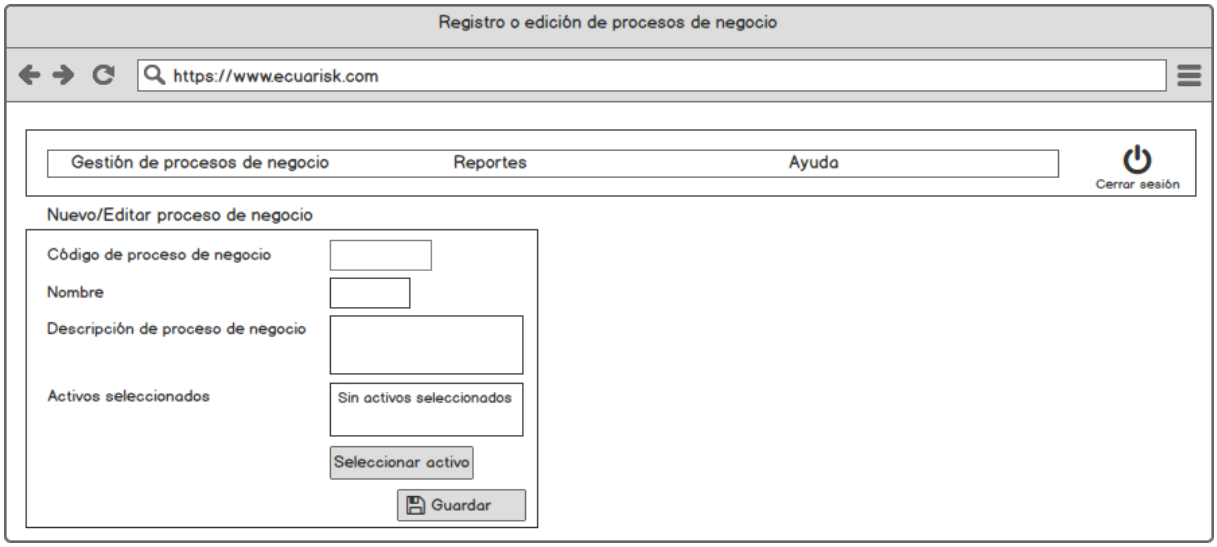

Ilustración 151: Interfaz de registro o edición de procesos de negocio.
Fuente: Elaboración propia.

La ilustración 152 representa el registro o edición de información de procesos de negocio, con la ventana emergente de selección de activos de información.

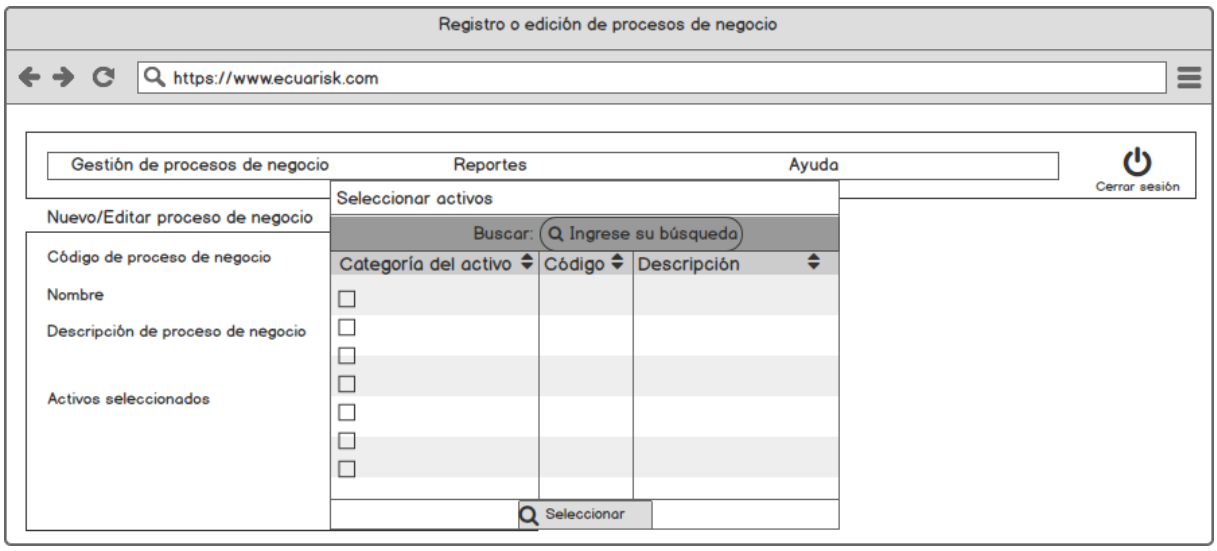

Ilustración 152: Interfaz de registro o edición de procesos de negocio con selección de activos.
Fuente: Elaboración propia.

La ilustración 153 representa la interfaz gráfica de consulta de los procesos de negocio, registrados en el sistema, el ícono ℹ representa el acceso a los detalles del proceso de negocio, el ícono ✎ representa el acceso a editar la información del proceso de negocio.

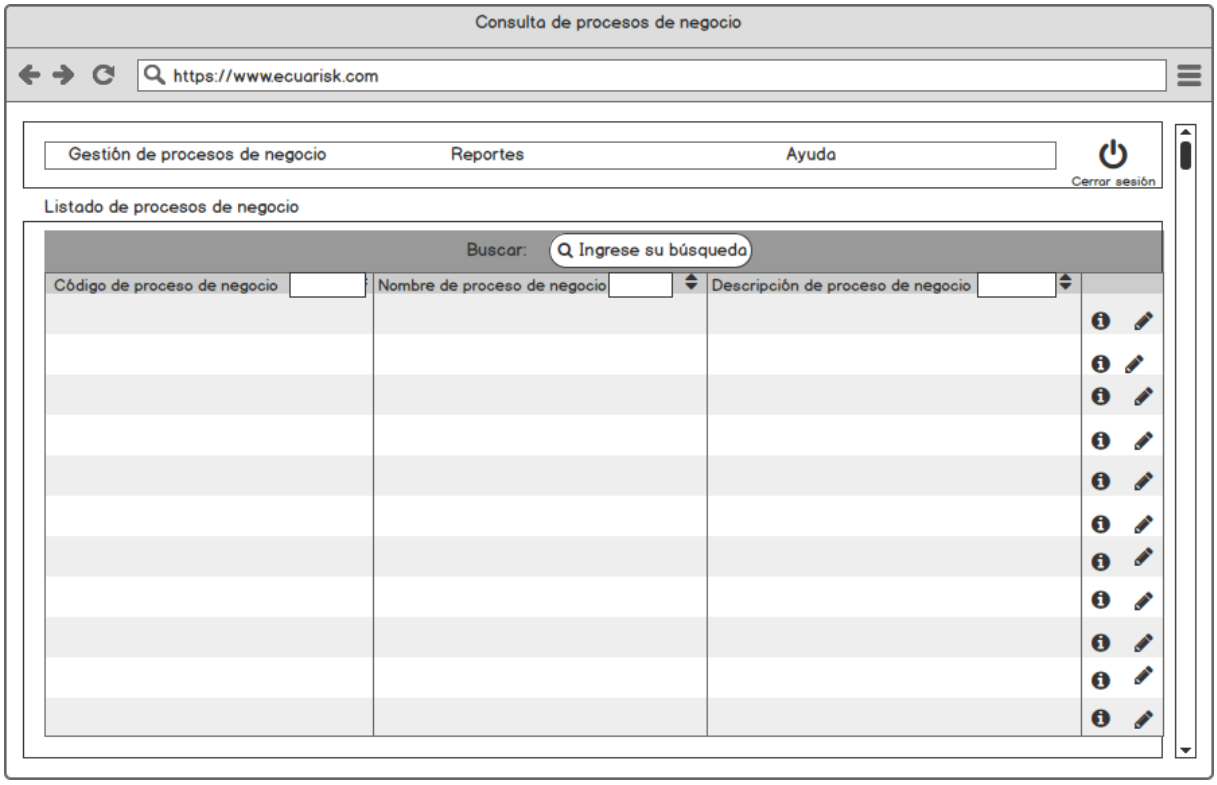

Ilustración 153: Interfaz de consulta de procesos de negocio.
Fuente: Elaboración propia.

La ilustración 154 representa la interfaz de consulta de detalles de un proceso de negocio.

Ilustración 154: Interfaz de consulta de detalles de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 155 representa la interfaz de registro o edición de información de una baja o alta de un proceso de negocio.

Ilustración 155: Registro o edición de baja o alta de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 156 representa la interfaz de registro o edición de baja o alta de un proceso de negocio, con la ventana emergente de selección de proceso de negocio.

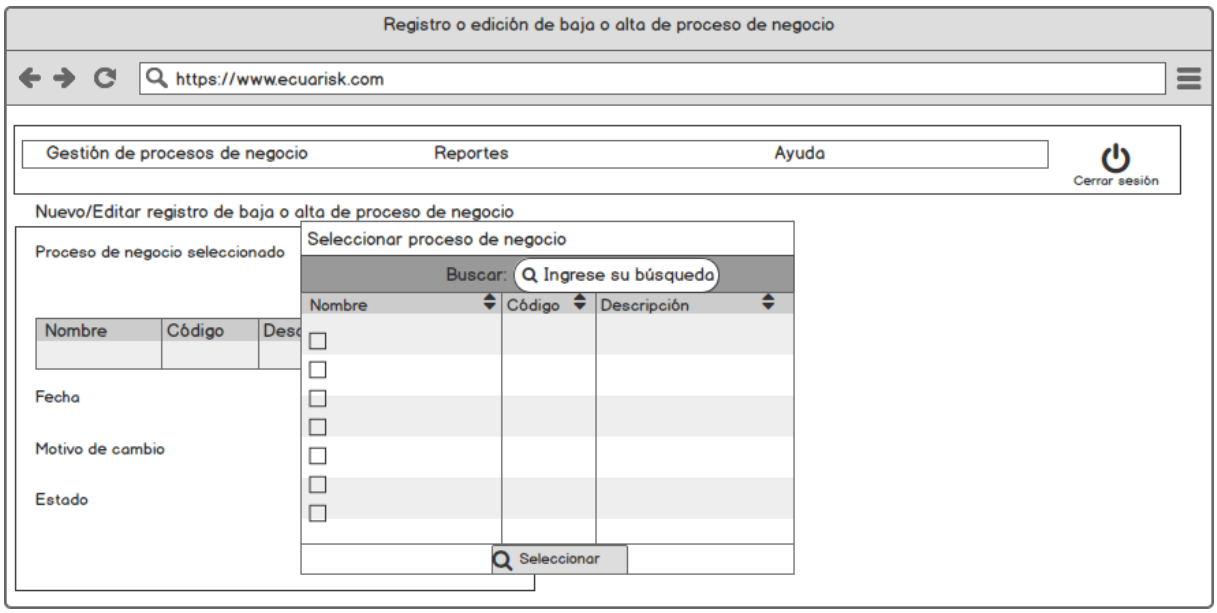

Ilustración 156: Registro o edición de baja o alta de proceso de negocio con ventana de selección de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 157 representa la interfaz de consulta de los registros de alta o baja de procesos de negocio, el ícono ✎ representa el acceso a editar la información del registro.

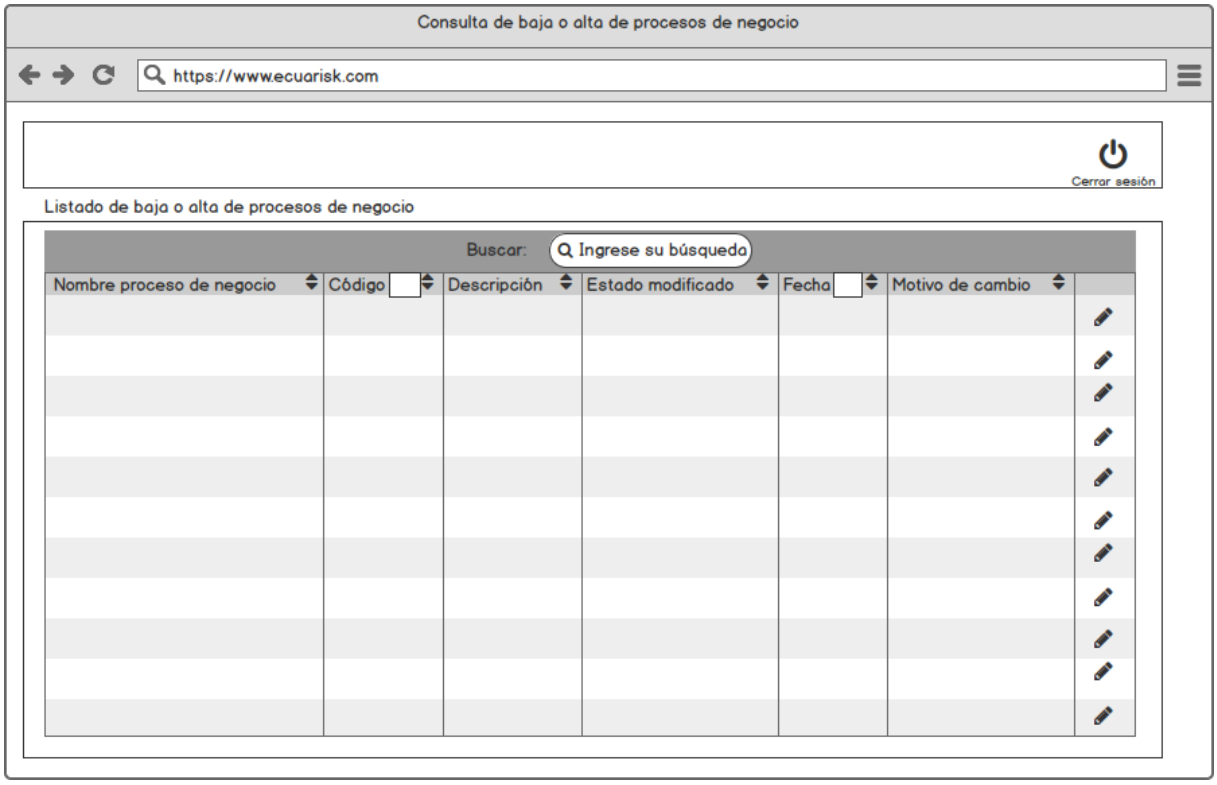

Ilustración 157: Consulta de baja o alta de procesos de negocio.
Fuente: Elaboración propia.

La ilustración 158 representa la interfaz gráfica del registro o edición de información de un seguimiento de un proceso de negocio.

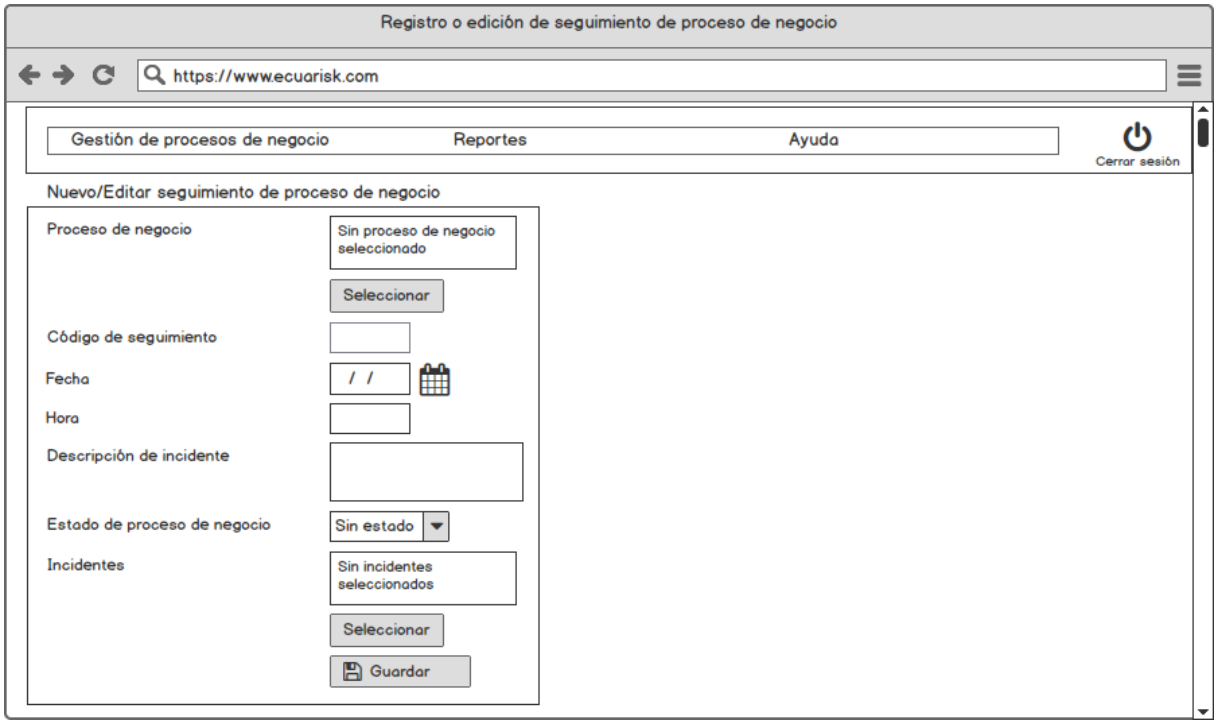

Ilustración 158: Interfaz de registro o edición de seguimiento de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 159 representa la interfaz gráfica del registro o edición de información de un seguimiento de un proceso de negocio, con la ventana emergente de selección de proceso de negocio afectado.

Ilustración 159: Interfaz de registro o edición de seguimiento de proceso de negocio con selección de proceso de negocio.
Fuente: Elaboración propia.

La ilustración 160 representa la interfaz gráfica del registro o edición de información de un seguimiento de un proceso de negocio, con la ventana emergente de selección de incidentes.

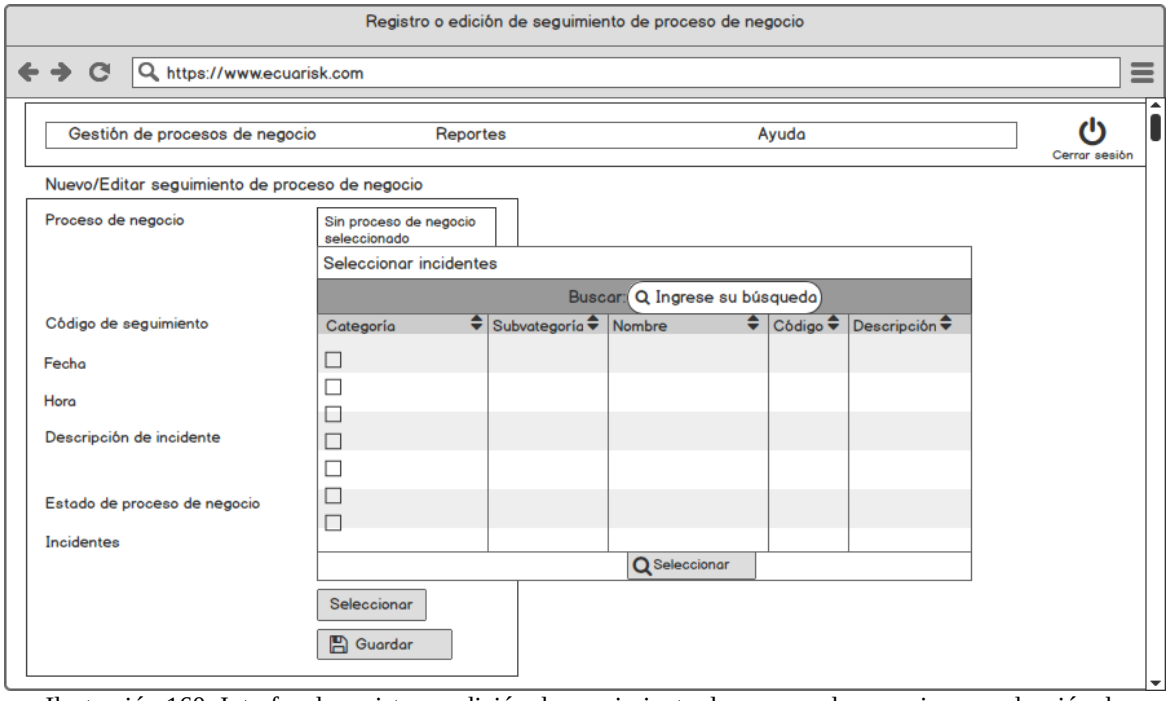

Ilustración 160: Interfaz de registro o edición de seguimiento de proceso de negocio con selección de incidentes.
Fuente: Elaboración propia

La ilustración 161 representa la consulta de los seguimientos de procesos de negocio en el sistema, el ícono ℹ representa el acceso a los detalles del seguimiento de proceso de negocio, el ícono ✎ representa el acceso a editar la información del seguimiento de proceso de negocio.

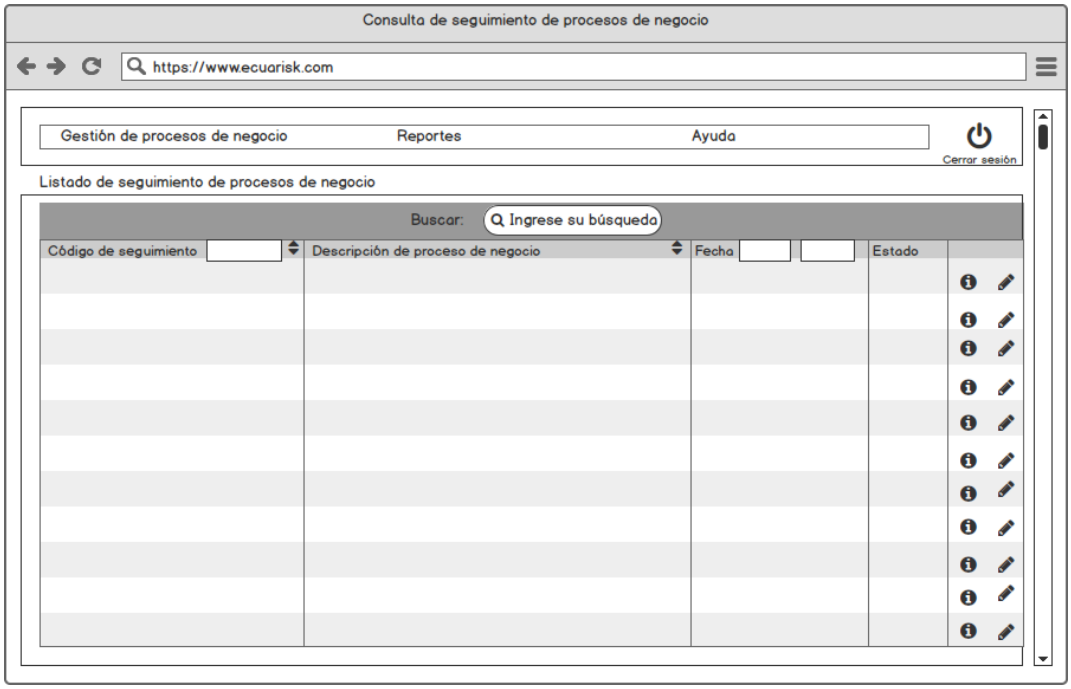

Ilustración 161: Consulta de seguimientos de procesos de negocio.
Fuente: Elaboración propia.

La ilustración 162 representa la consulta de los detalles de un seguimiento de un proceso de negocio.

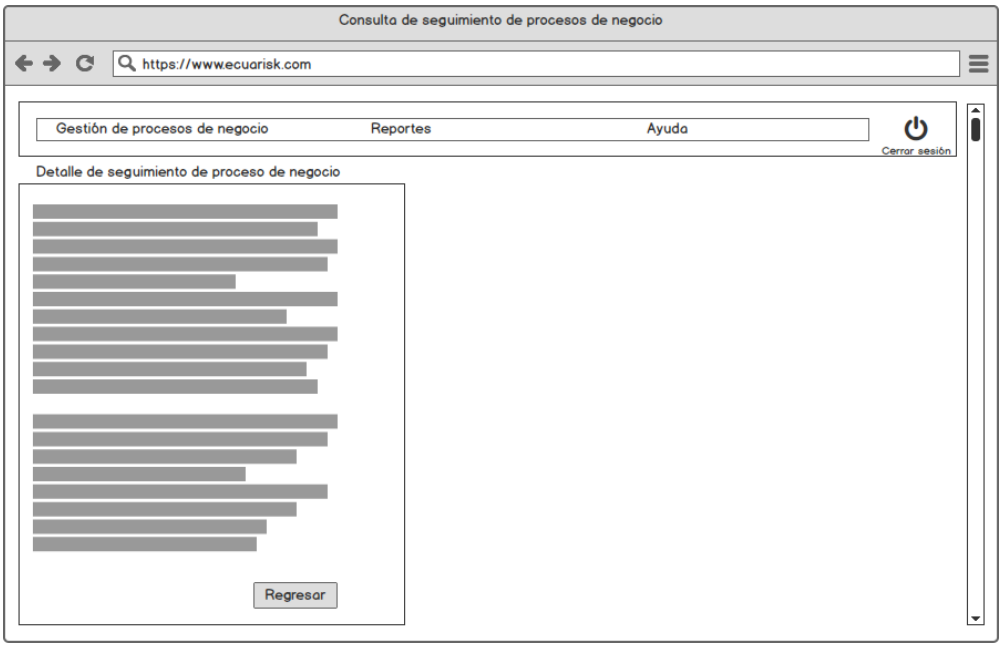

Ilustración 162: Consulta de detalles de seguimiento de un proceso de negocio.
Fuente: Elaboración propia.

La ilustración 163 representa a la interfaz gráfica del reporte cuadro de mando integrado.

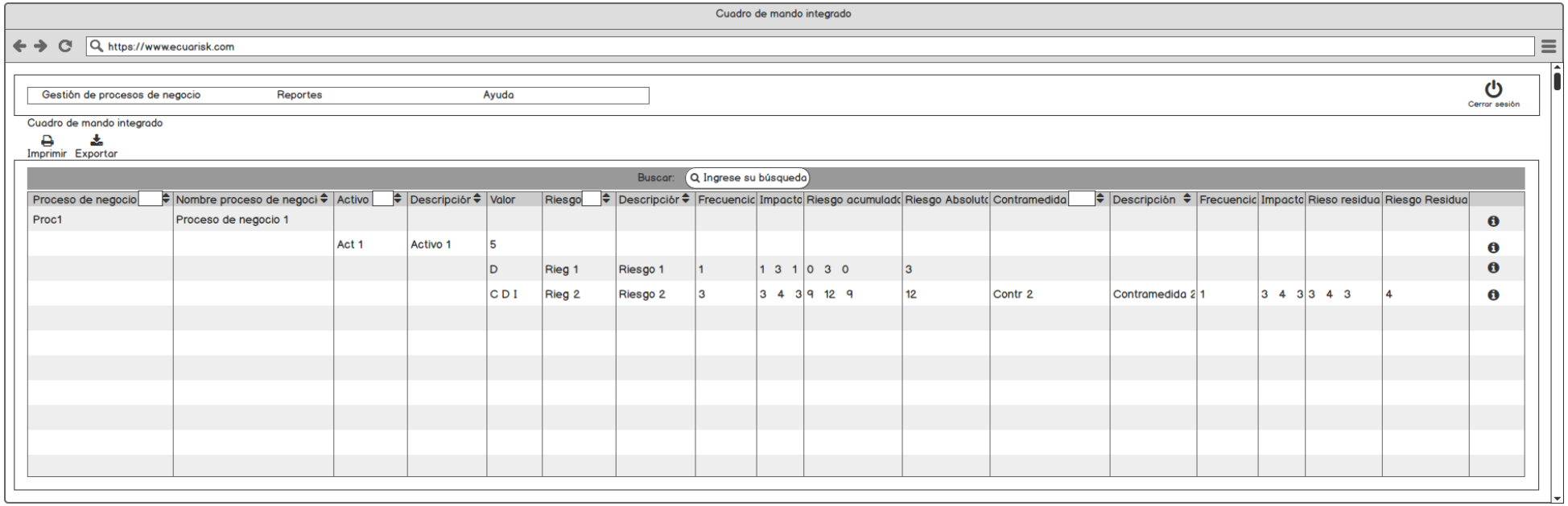

Ilustración 163: Interfaz de reporte cuadro de mando integrado.
Fuente: Elaboración propia.

La ilustración 164 representa la interfaz gráfica del reporte de indicador clave de desempeño de incidentes.

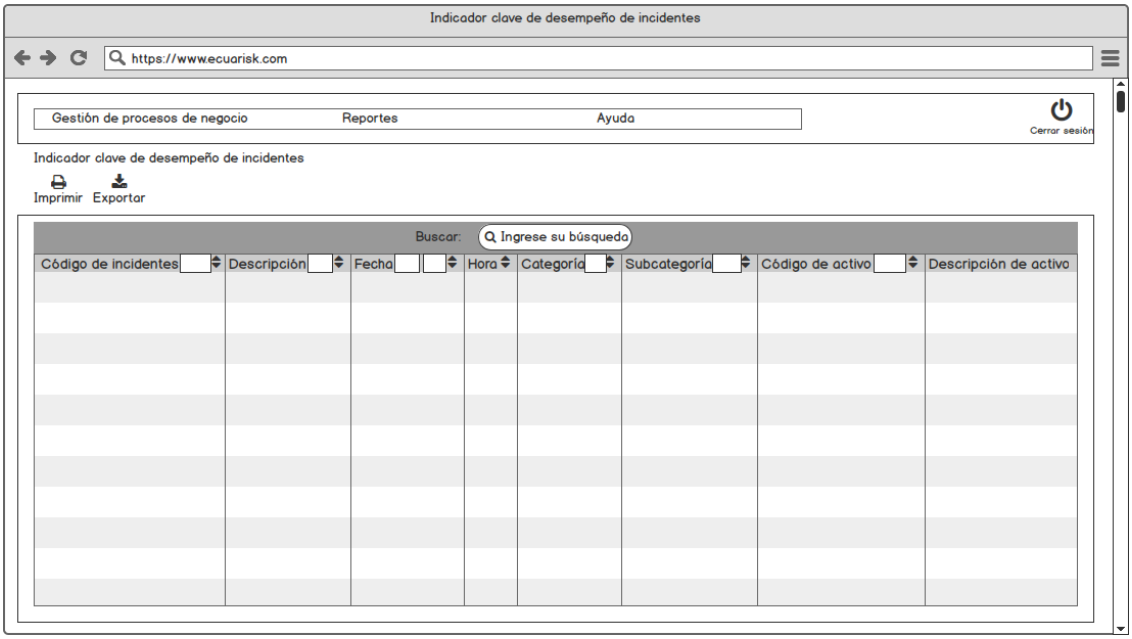

Ilustración 164: Interfaz de reporte de indicador clave de desempeño de incidentes.
Fuente: Elaboración propia.

La ilustración 165 representa la interfaz gráfica del reporte de indicador clave de desempeño de planes de tratamiento.

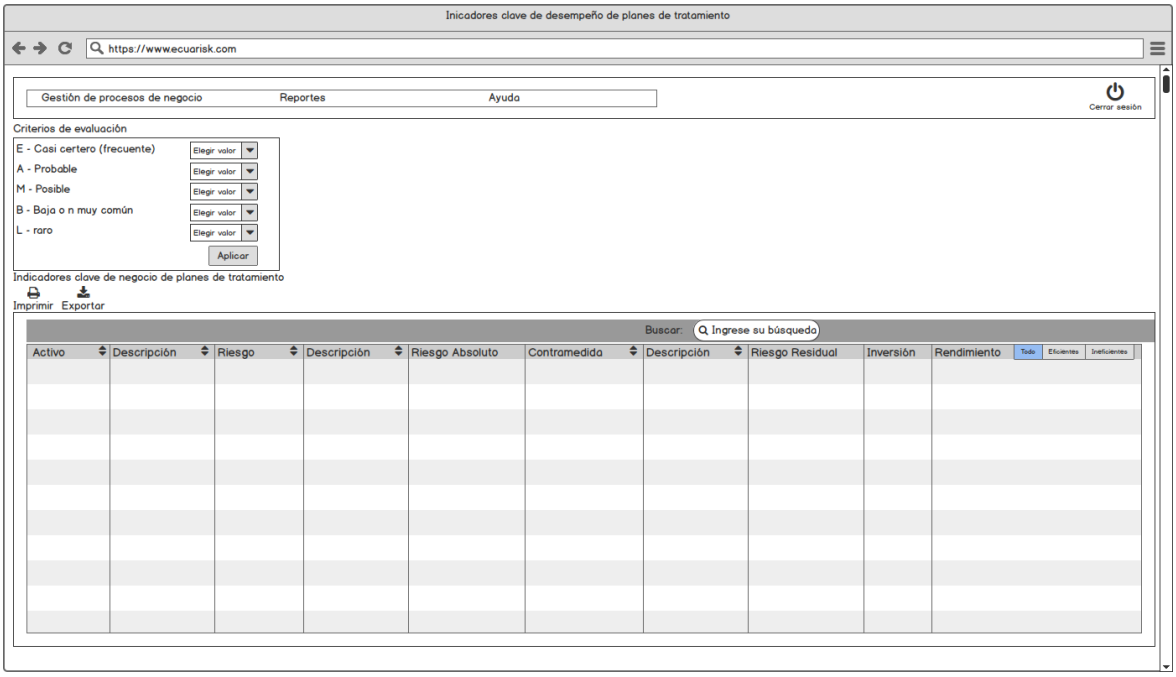

Ilustración 165: Interfaz de reporte de indicador clave de desempeño de planes de tratamiento.
Fuente: Elaboración propia.

La ilustración 166 representa la interfaz gráfica del reporte de indicadores clave de desempeño de procesos de negocio.

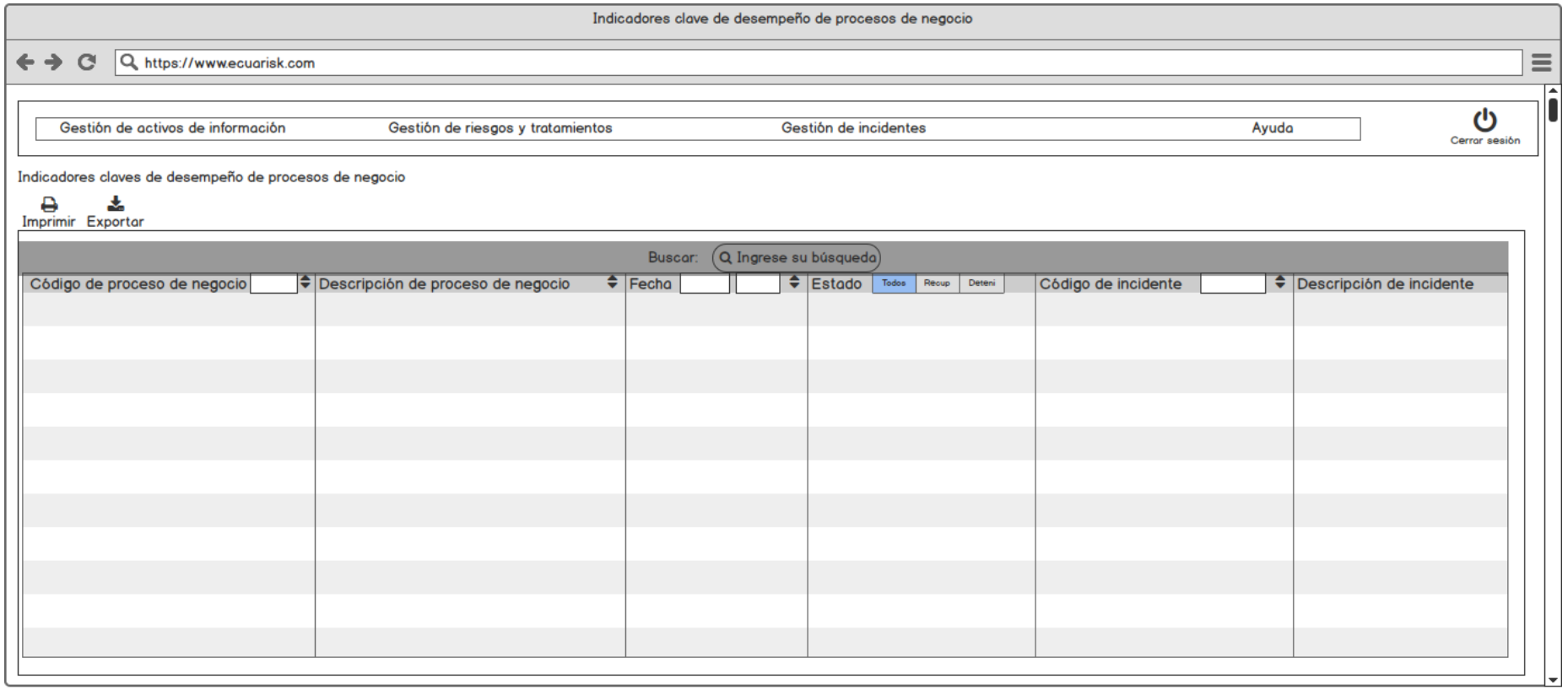

Ilustración 166: Interfaz de indicadores claves de desempeño de procesos de negocio.
Fuente: Elaboración propia.

La ilustración 167 representa la interfaz gráfica de registro o edición de usuario.

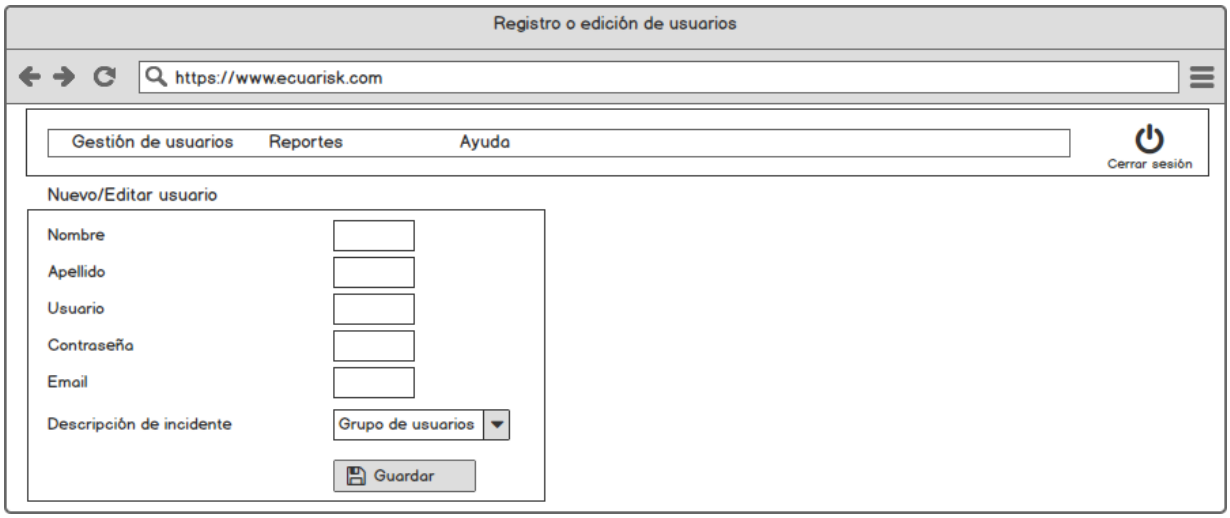

Ilustración 167: Registro o edición de usuario.
Fuente: Elaboración propia.

La ilustración 168 representa la consulta de usuarios en el sistema, el ícono ℹ representa el acceso a los detalles del usuario, el ícono ✎ representa el acceso a editar la información usuario.

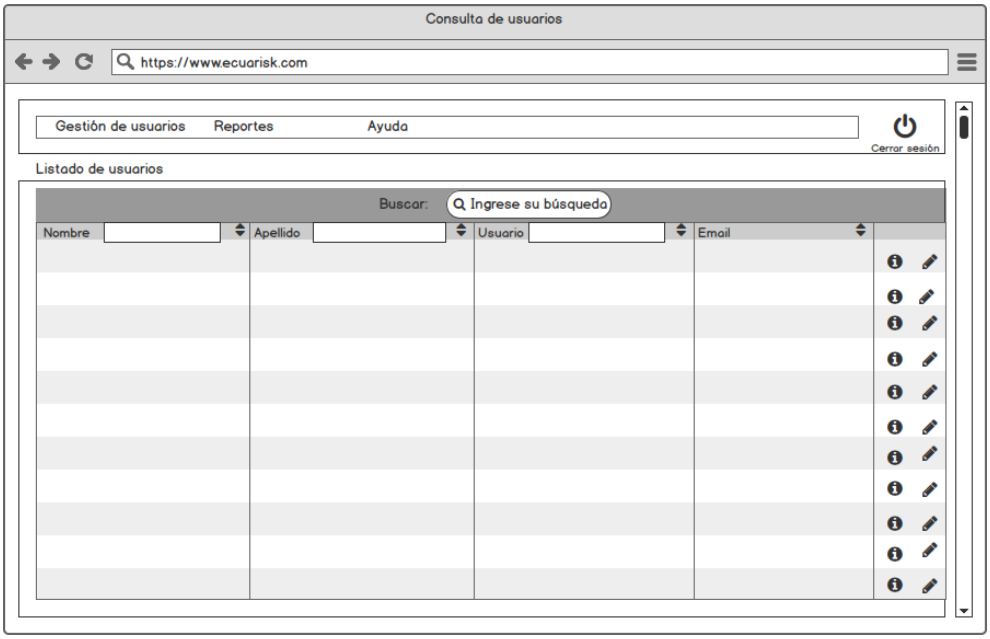

Ilustración 168: Consulta de usuarios.
Fuente: Elaboración propia.

La ilustración 169 representa la consulta de los detalles de usuario.

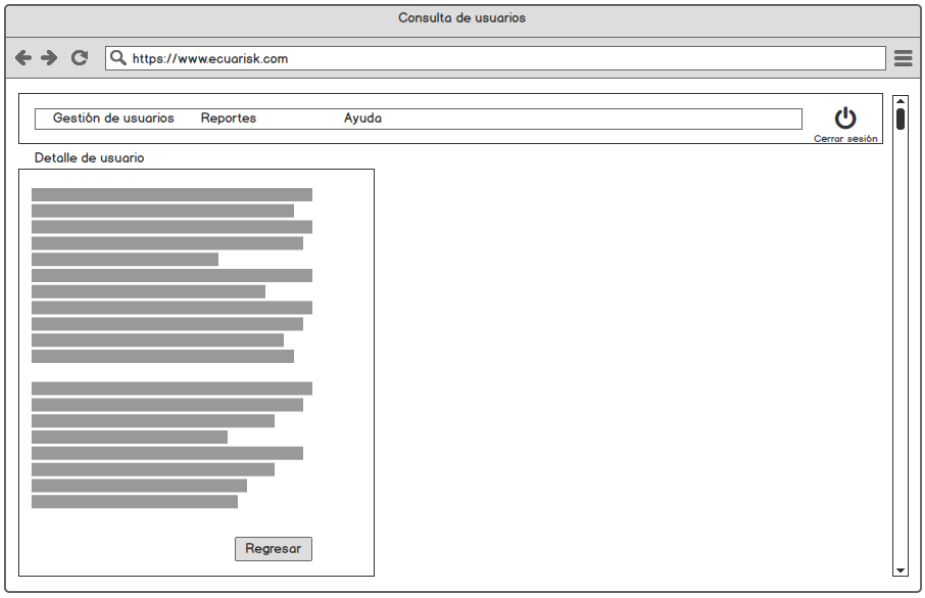

Ilustración 169: Consulta de detalles de usuario.
Fuente: Elaboración propia.

4.8. Diseño arquitectónico

4.8.1 Arquitectura de contenido

El sistema de gestión de riesgos Ecu@Risk, se basará en una estructura global en red, dicha estructura también es conocida como "Web pura" debido a su uso común en la nube, este diseño de estructura permite navegar por medio de vínculos de hipertexto a cualquier parte del sistema. (García Chi, 2013).

Como se ha visto en el diseño de interfaz presentado anteriormente, cada usuario puede desplazarse en el sistema mediante el uso del menú de navegación.

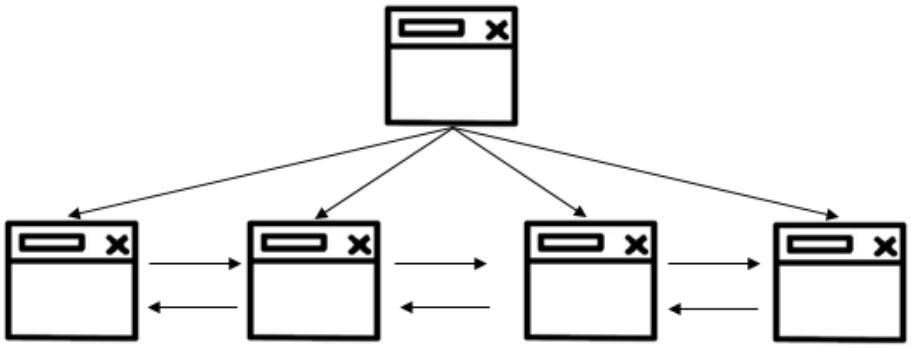

Ilustración 170: Estructura en red.
Fuente: Elaboración propia.

4.8.2. Arquitectura de aplicación Web

En este apartado se describe la arquitectura que va a ser adoptada por el sistema web Ecu@Risk. De acuerdo al diseño establecido y la estructura de navegación propuesta, la arquitectura elegida para el sistema es el Modelo Vista Controlador (MVC).

Se toman los conceptos del MVC del servicio de informática de la Universidad de Alicante (2018), MVC es un modelo común para los sistemas y aplicaciones web, esta arquitectura separa la interfaz del usuario, la funcionalidad del sistema y el contenido de la información.

Modelo: es el encargado de acceder a los datos, contenido de la aplicación o sistema y la lógica de procesamiento (reglas de negocio).

Vista: se refiere a la interfaz de usuario, contiene funciones específicas para la interacción entre el usuario y la interfaz, también es el encargado de recibir los datos enviados desde el modelo y mostrarlos al usuario.

Controlador: es el intermediario entre la Vista y el Modelo, coordinando el flujo de información entre ambos. Es decir, el controlador es quien recibe las órdenes del usuario, solicita los datos al Modelo y se los comunica a la Vista.

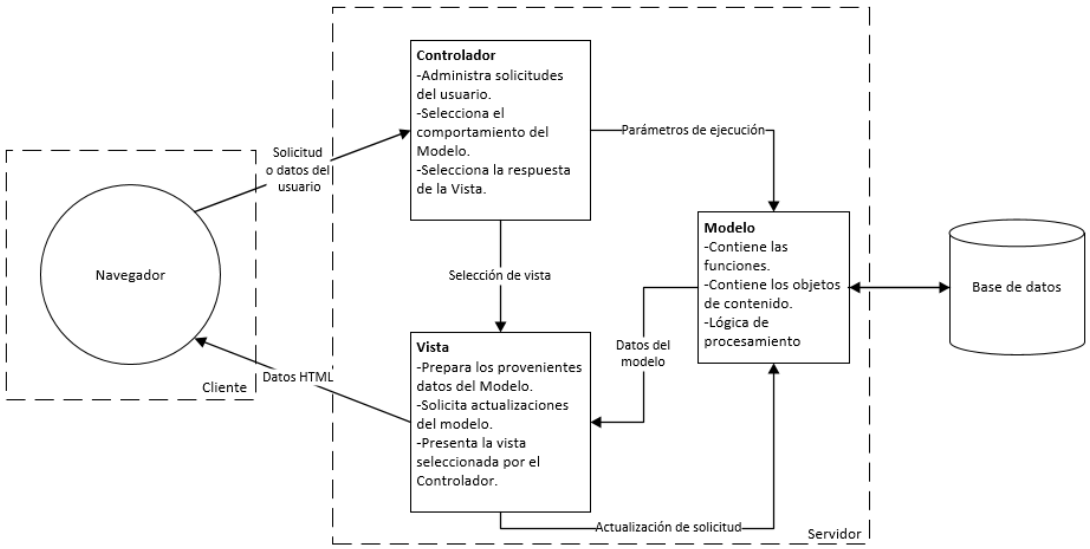

Ilustración 171: Arquitectura MVC para el sistema Ecu@Risk.
Fuente: Elaboración propia.

El Modelo Vista Controlador se ha convertido en una arquitectura muy apetecida en entornos de desarrollo web, la misma ha sido probada y funciona muy bien en este ambiente. Con este tipo de arquitectura el sistema se podrá desarrollar rápidamente, de manera modular, lo que hará que mantenerlo sea una tarea más sencilla.

Al separar al sistema en modelos, vistas y controladores hace que el mismo sea más ligero. Un sistema web cuando es modular permite a los desarrolladores y diseñadores trabajar conjuntamente, lo que hace que el sistema pueda ser diseñado e implementado de manera más rápida, al hacerlo modular permite realizar cambios en cualquier parte del sistema sin que las demás partes se vean comprometidas en funcionamiento.

Estas son las razones por la cual el sistema Ecu@Risk debe manejar la arquitectura MVC.

4.9. Diseño de base de datos

La base de datos es un recurso muy importante de la empresa, ya que es el lugar en donde se almacena toda la información valiosa de la organización, por lo tanto, se busca siempre que una base de datos tenga un diseño que garantice su eficacia, rapidez y agilidad.

La base de datos del sistema de gestión de seguridad de la información Ecu@Risk, ha sido diseñada siguiendo y utilizando los conceptos del modelo Entidad Relación (E-R) los cuales son: entidades, relaciones y atributos; llegando a conseguir un diseño de una base de datos relacional, misma que facilita la normalización de los datos, evita la duplicidad en los registros, asegura la integridad referencial de los registros, presenta atomicidad entre las transacciones de la base de datos (Rollback), entre otras propiedades; estas características de la base de datos relacional, representan reducción de errores y el espacio de almacenamiento. (Kendal, 2011)

El diseño de la base de datos fue realizado en la herramienta MySQLWorkbench, que es una herramienta visual unificada que permite diseñar y modelar datos, desarrollar SQL, administrar y mantener bases de datos que se basen en el sistema de gestión de bases de datos relacionales MySQL. (MySQL, s.f.)

A continuación, se presenta el diagrama Entidad Relación de base de datos del sistema de gestión de seguridad de la información Ecu@Risk.

4.9.1. Diagrama Entidad Relación de base de datos del sistema Ecu@Risk

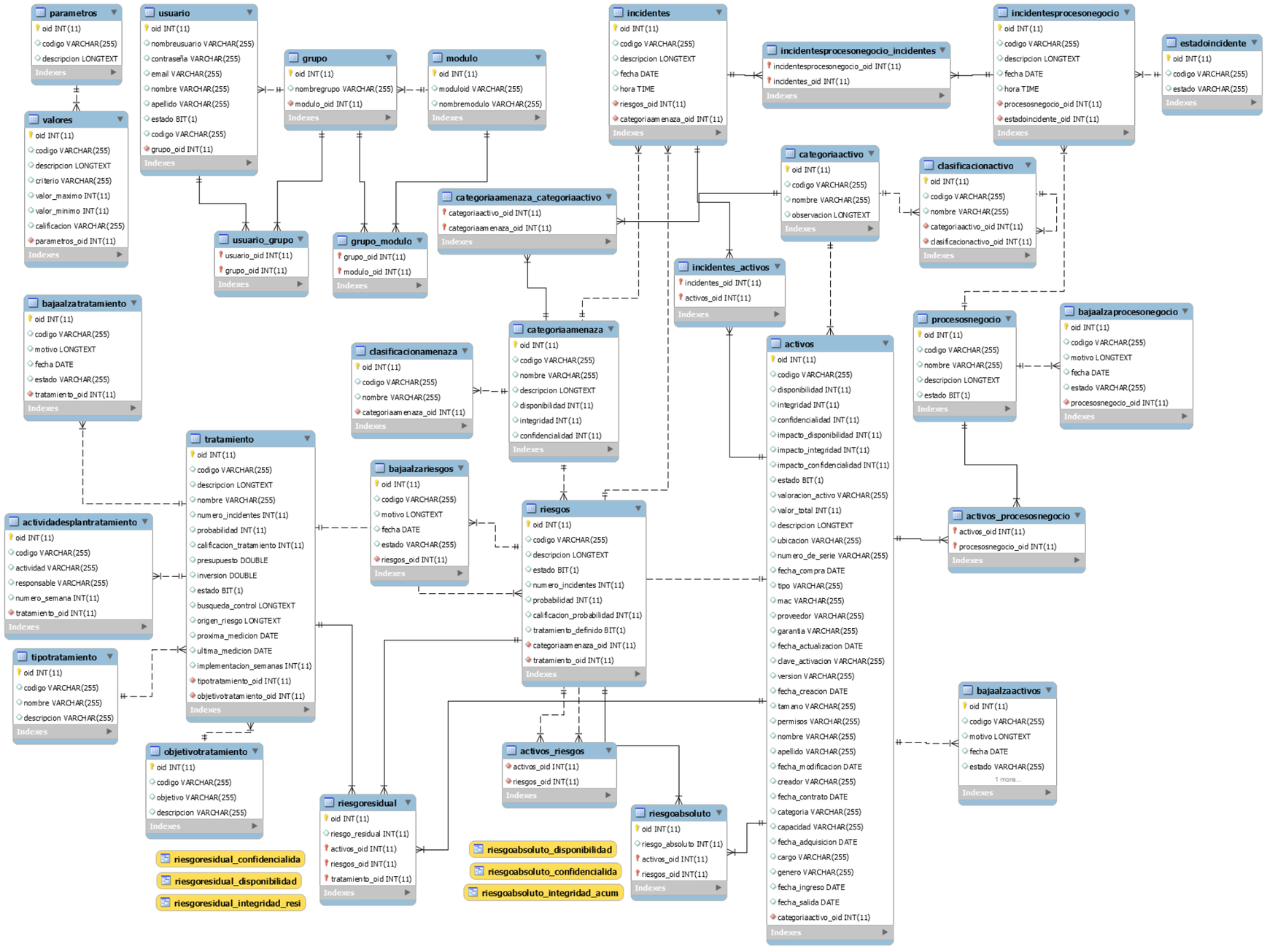

Ilustración 172: Diagrama entidad relación sistema Ecu@Risk
Fuente: Elaboración propia.

4.10. Conclusiones del capítulo 4

La aplicación del modelo de análisis para aplicaciones web, facilitó el análisis y diseño del sistema de seguridad de la información Ecu@Risk, seguir los modelos y análisis para desarrollo de aplicaciones y sistemas web permitió elaborar un amplio y completo sistema el cual fue desarrollado conforme a los requerimientos levantados para el sistema en capítulos anteriores.

El modelo de contenido se representa a través de los diagramas de clase utilizando el lenguaje unificado de modelado (UML), las clases representan a los elementos estructurales que forman el sistema, estos elementos estructurales son las entidades visibles y manipulables para el usuario a través del sistema, fueron implementados a partir de un análisis minucioso de los casos de uso presentados en los requerimientos del sistema.

El modelo de interacción fue representado a través de los diagramas de secuencia utilizando el lenguaje unificado de modelado (UML), se representó la interacción entre el usuario y cada una de las partes del sistema a través de una línea de tiempo, es decir, se definió cómo será el comportamiento del sistema ante las acciones del usuario.

El modelo funcional, que representa la funcionalidad del sistema hacia el usuario, se lo hizo mediante diagramas de actividades utilizando el lenguaje unificado de modelado (UML), es decir, todo lo que el usuario puede realizar en el sistema.

El modelo de configuración se lo utilizó para especificar las características y relaciones entre hardware y software que se utilizarán en el sistema de gestión de seguridad de la información Ecu@Risk, es decir, es la configuración del sistema.

El análisis de relación navegación (ARN), se utilizó para identificar cada uno de los elementos que conforma el sistema y cómo se relacionan entre ellos y cómo los usarán cada uno de los usuarios; así mismo, sirvió para hacer una planificación de cómo será la navegación del usuario dentro del sistema.

El diseño de interfaz se realizó mediante el uso mockups, que son una representación de la interfaz gráfica del sistema; para ello se utilizó varios íconos estandarizados para hacer que el usuario no tenga inconvenientes para familiarizarse con la funcionalidad de cada parte del sistema. Cada funcionalidad del sistema está explicada y es muy intuitivo para hacer que su uso sea sencillo para el usuario.

El diseño arquitectónico del sistema se lo analizó y escogió de acuerdo al análisis de relación navegación y diseño de interfaz realizado previamente. El diseño arquitectónico de contenido es una estructura en red, en la cual el usuario podrá navegar en el sistema a través de vínculos de hipertexto que se están en el menú principal de navegación de cada usuario, este menú se presenta en todas las interfaces gráficas del sistema, por lo tanto, el usuario puede acceder a cualquier sección del sistema desde el punto en el que se encuentre. El modelo arquitectónico elegido para el sistema es el Modelo Vista Controlador (MVC), un modelo que es muy utilizado en aplicaciones y sistemas de tipo web; este modelo permite que el sistema sea modular, lo que se significa que se puede ser desarrollado, implementado y mantenido una forma más sencilla y eficaz.

Son muchos los beneficios de la utilización de una base de datos relacional dentro de un sistema, como evitar la duplicidad de los datos, la atomicidad, integridad referencial de los datos, son más baratos y mayoritarios en el mercado, las herramientas de administración y gestión de la base de datos tienen un mayor soporte y cada vez salen mejores suites y complementos, etc. La empresa se ve muy favorecida al implementar este tipo de base de datos porque reduce errores en su funcionamiento y espacio de almacenamiento de los datos.

Capítulo 5: Gestión de proyecto

5.1. Introducción

La gestión de proyectos según el autor Gómez Rueda (2016), es la planificación y ejecución de un proyecto con la ayuda de conocimientos, métodos, herramientas, técnicas, etc., para el desarrollo del mismo. Esto se lo realiza para obtener un producto el cual satisfaga a todas las partes interesadas en él.

En este apartado se centrará en planificar y gestionar el desarrollo del sistema Ecu@Risk, siendo como punto principal la elección de la mejor metodología con la cual se pueda elaborar el sistema.

5.2. Metodologías de desarrollo

Para gestionar el proyecto de desarrollo del sistema se analizarán dos tipos de metodologías que son utilizadas en el desarrollo de software.

5.2.1. Metodologías tradicionales

Las metodologías tradicionales de desarrollo de proyectos de software, son orientadas a la planificación del mismo, es decir, se realiza una exhaustiva recopilación de los requisitos del software, previo a las etapas de análisis y diseño. Este tipo de metodología trabaja siempre dentro de un tiempo y un presupuesto. (Navarro Cadavid, Fernández Martínez, & Morales Vélez, 2013)

Las metodologías tradicionales elaboran un proyecto de gran dimensión con una estructura definida, es decir, la ejecución del proyecto será unidireccional y no deben cambios en los requisitos del mismo, si existe algún cambio, el mismo deberá pasar por un proceso y deberá ser aprobado por un comité de cambio. Por esta razón los requisitos requieren una gran cantidad de tiempo y esfuerzo, una vez acordados con el cliente son fijados para todo el proyecto. (Navarro Cadavid, Fernández Martínez, & Morales Vélez, 2013)

5.2.2. Metodologías ágiles

Las metodologías ágiles están orientadas a la ejecución del proyecto, este tipo de metodología nació de la necesidad de solucionar los problemas que las metodologías tradicionales no podían como el cliente las requería, ya que el cliente requería el software lo más pronto posible. Este tipo de metodología se caracteriza por su flexibilidad ante los cambios

que se requieren durante la elaboración del software solicitados por parte del cliente, además el equipo de trabajo es pequeño y auto-gestionado, suelen subdividir el proyecto y trabajar en pequeñas partes del software para realizar una constante entrega del mismo al cliente, para garantizar su satisfacción y calidad del producto final. El cliente tiene una participación constante y activa en el desarrollo del proyecto. (Navarro Cadavid, Fernández Martínez, & Morales Vélez, 2013)

5.2.3. Comparación entre metodologías

En la siguiente tabla los autores Navarro Cadavid, Fernández Martínez y Morales Vélez (2013) señalan los aspectos más importantes de cada metodología y se los comparan.

Tabla 53:
Comparación entre metodologías tradicionales y ágiles.

Metodologías tradicionales	Metodologías ágiles
Predictiva.	Adaptativa.
Orientada a procesos.	Orientada a personas.
Proceso rígido.	Proceso flexible.
Se concibe como un proyecto.	Un proyecto es subdividido en varios proyectos más pequeños.
Poca comunicación con el cliente.	Constante comunicación con el cliente.
Entrega de software al finalizar el desarrollo.	Entregas constantes de software.
Documentación extensa.	Poca documentación.

Fuente: (Navarro Cadavid, Fernández Martínez, & Morales Vélez, 2013)

Ninguna de las dos metodologías es mejor que la otra, sino representan diferentes proyectos, la una representa más la planificación para entregar un producto de calidad, y la otra se basa en la ejecución del proyecto para poder entregar el producto lo antes posible, y satisfacer al cliente.

Para el desarrollo del sistema de gestión de seguridad de la información Ecu@Risk, se opta por desarrollarla con una metodología ágil. Debido a que se requerirá tenerlo desarrollado e implementado de manera rápida para que las empresas MPYMES gestionen sus activos y riesgos lo antes posible. El software puede presentar modificaciones o implementaciones de

requerimientos, debido a algún cambio en la construcción; la metodología que se adapta mejor a los requisitos de desarrollo del sistema es una metodología ágil.

5.3. Metodología de desarrollo del sistema Ecu@Risk

La metodología elegida para desarrollar el sistema Ecu@Risk es SCRUM, debido a que en la actualidad es la metodología de desarrollo más conocida, utilizada y confiable en la gestión de proyectos de desarrollo de software. Esta metodología es fácilmente implementable en cualquier equipo de desarrollo y la probabilidad éxito proyecto es muy grande. SCRUM aporta ciertas características al proyecto como: la agilidad en su desarrollo, garantizar una alta calidad de software, equipos de trabajo unidos, facilidad de escalabilidad, etc. En la actualidad varias empresas de renombre a nivel mundial implementan SCRUM para desarrollar sus proyectos como: Spotify, Adobe, Google, entre otras.

5.4. SCRUM

La metodología SCRUM es un marco de trabajo para el desarrollo ágil de software que ha sido elaborado para conseguir la colaboración y compromiso de los equipos de desarrollo; se centra en el desarrollo iterativo (Sprints) e incremental; esta metodología define reglas a seguir, requiere de ciertos artefactos y el establecimiento de roles para su correcta aplicación y funcionamiento. (Navarro Cadavid, Fernández Martínez, & Morales Vélez, 2013)

5.4.1. El equipo SCRUM (Scrum Team)

Los autores Schwaber y Sutherland (2013) en su guía de SCRUM definen tres roles principales para la gestión del desarrollo del proyecto:

- **Dueño del producto (Product Owner):** es la persona encargada de tomar las decisiones en el proyecto, es el encargado de dar valor al producto debido a que es él quien tiene conocimiento del negocio del cliente; es el encargado de gestiona la lista del producto (Product Backlog) y cualquier cambio que se requiera en el producto deberá pasar por el dueño del producto.
- **Equipo de desarrollo (Development Team):** es el grupo de personas encargadas de transformar lo que el cliente quiere, es decir, la lista del producto en iteraciones funcionales y entregables, en el equipo de desarrollo no existe ninguna jerarquía cada uno es desarrollador, sin embargo, pueden existir miembros especializados en

diferentes áreas, pero se juzga al equipo como uno solo. La cantidad de un equipo de desarrollo óptimo va desde 3 personas hasta 9.

- **Scrum Master:** es el administrador del proyecto, encargado de garantizar que la metodología y el modelo esté funcionando en el equipo de trabajo. También se encarga de proporcionar las herramientas necesarias para las iteraciones fluyan en el proceso de elaboración del producto, se encarga también de organizar las reuniones, también interactúa con el cliente.

Schwaber y Sutherland (2013) indican en su guía que hay personas que son necesarias y forman parte de la retroalimentación del proceso de Scrum, con esta información se plantea y modifica cada Sprint:

- **Usuarios:** son a quienes van dirigido el producto final.
- **Stakeholders:** se definen como las personas a las que la elaboración del proyecto les dará algún rédito, incluso invierten económicamente para su desarrollo. Los interesados del proyecto intervienen en las revisiones de cada Sprint.

Este equipo de trabajo debe ser auto-organizado y multifuncionales, es decir, nadie externo al equipo los dirige, sino que ellos mismo eligen la forma de llevar acabo su trabajo; al igual que no deben depender de nadie externo al equipo para realizar las tareas, sino el equipo está en la completa capacidad de llevar acabo el trabajo. El equipo Scrum realiza la entrega del producto de forma iterativa, en cada iteración crea o modifica funcionalidades del producto conforme las solicite el dueño del producto. (Schwaber & Sutherland, 2013)

5.4.2. Artefactos de Scrum

Los autores Schwaber y Sutherland (2013) en su guía de Scrum definen los siguientes artefactos de la metodología:

- **Lista del producto (Product Backlog):** es una lista ordenada con todos los requisitos o funcionalidades del producto, esta lista es manipulada únicamente por el dueño del producto con ayuda del Scrum master; esta lista será modificada y evolucionará de acuerdo como avance el proyecto.
- **Sprint Backlog:** Es la lista de tareas que se realizará en una iteración o Sprint por parte del equipo de desarrollo, en esta lista pueden tener tareas rezagadas de un Sprint anterior, y se lo realizará de acuerdo a su prioridad.

- **Incremento:** representa a las partes del producto que se han "terminado" en el Sprint y que son funcionales en su totalidad.

5.4.3. Eventos de Scrum

Los autores Schwaber y Sutherland (2013) en su guía de Scrum definen los siguientes eventos, los cuales son definidos con el objetivo de minimizar las reuniones no definidas.

¿Qué es un sprint?

Scrum está basada en el método de iteración, por esta razón un Sprint se convierte en el corazón de esta metodología. El Sprint es un bloque de tiempo (time-box), que puede ir desde días hasta máximo un mes, se desarrollará una parte incremental del producto, la cual se considerará una versión utilizable del mismo y se lo presentará al dueño del producto. Un Sprint siempre empieza con la finalización de uno anterior, las tareas que no fueron concluidas en el Sprint planificado pueden ser relegadas al siguiente Sprint y se las ejecuta de acuerdo a su nivel de prioridad.

Cada Sprint cuenta con eventos específicos que se los detallará a continuación:

- **Planificación (Sprint Planning Meeting):** Es una reunión antes del inicio del Sprint en donde se muestran los objetivos a alcanzar y el trabajo a realizar durante el desarrollo de esa iteración. Esta planificación la realiza el equipo Scrum conjuntamente. Cuando un Sprint dura un mes esta reunión dura 8 horas, cuando el Sprint es de menor tiempo, la reunión durará menos también.
- **Reunión diaria (Daily Scrum):** Es una reunión diaria que se da mientras está en desarrollo el Sprint. Tiene una duración aproximada de quince minutos, en la cual participa el Scrum Master con el equipo de desarrollo; esta reunión sirve para que el equipo de desarrollo comunique cuáles son las tareas terminadas desde la última vez que se dio a cabo esta reunión, también exponen si surgió algún inconveniente y se lo intenta solucionar inmediatamente.
- **Revisión (Sprint Review Meeting):** Es una reunión que se realiza al finalizar el Sprint entre todo el equipo de Scrum y todos los interesados en el producto; esta reunión dura alrededor de 4 horas si fue un Sprint de un mes, si duró menos el Sprint será proporcionalmente menor; en esta reunión se exponen todas las tareas culminadas e incrementadas al producto final, también se exponen todos los inconvenientes surgidos

y la manera en que se solucionaron los problemas, si existen tareas no culminadas el Sprint Block es modificado por el dueño del producto; esta reunión es muy importante para los siguientes Sprints.

- **Reunión de retrospectiva (Sprint Restrospective):** Se reúne el equipo Scrum, y analizan el desempeño en el Sprint que está cerrando; se analizan ciertos aspectos como la comunicación, los procesos de la metodología, las herramientas, etc. También se analizan aspectos positivos y errores detectados, lo que permite desarrollar un plan de mejoras para el siguiente Sprint. La duración de esta reunión para un mes de desarrollo es de 3 horas; si el Sprint duró menos, el espacio para esta reunión también será proporcional.

5.5. Lista del producto (Product Backlog) del sistema Ecu@Risk

Los requerimientos del sistema Ecu@Risk fueron levantados, pero no valorizados, en este apartado se elaborará la lista del producto donde se ponderará la prioridad y la complejidad de los mismos a través de la siguiente tabla:

Tabla 54:
Tabla de ponderaciones.

Número	Prioridad	Complejidad
1	Baja	Fácil
2	Media	Medio
3	Alta	Complejo
4	Muy Alta	Muy complejo

Fuente: (Navarro Cadavid, Fernández Martínez, & Morales Vélez, 2013)

A continuación, se presenta la lista del producto del sistema, la cual tiene la prioridad, la complejidad de desarrollo.

Tabla 55:
Lista del producto del sistema Ecu@Risk.

Product Backlog			
ID	**Caso de uso**	**Prioridad**	**Complejidad**
1	Inicio de sesión	4	2
2	Autenticación Token	4	3
3	Pantalla de inicio de usuarios.	4	2
4	Registro de activos de información.	4	3

5	Consulta de activos de información.	4	2
6	Consulta detalle de activos de información.	4	1
7	Modificación de activos de información.	4	2
8	Registro de alta o baja de activos de información.	2	3
9	Consulta de alta o baja de activos de información.	2	2
10	Modificación de baja o alta de activos de información.	2	2
11	Registro de riesgos.	4	3
12	Consulta de riesgos.	4	2
13	Consulta de detalles de riesgos.	4	1
14	Modificación de riesgos.	4	2
15	Relación de activos con riesgos.	4	3
16	Registro plan de tratamiento al riesgo.	4	3
17	Consulta de plan de tratamiento.	4	2
18	Consulta detalle de plan de tratamiento.	4	1
19	Modificar de plan de tratamiento.	4	2
20	Imprimir plan de tratamiento.	3	2
21	Medición de plan de tratamiento.	4	3
22	Relación de activos con riesgos y planes de tratamiento.	4	3
23	Registro de alta o baja de riesgos.	2	3
24	Consulta de alta o baja de riesgos.	2	2
25	Modificación de baja o alta de riesgos.	2	2
26	Registro de alta o baja de planes de tratamiento.	2	3
27	Consulta de alta o baja de planes de tratamiento.	2	2
28	Modificación de baja o alta de planes de tratamiento.	2	2
29	Registro de incidentes.	4	3
30	Consulta de incidentes.	4	2
31	Consulta detalles de incidente.	2	1
32	Modificación de incidente.	4	1
33	Registro de procesos de negocio.	4	2
34	Consulta de procesos de negocio.	4	2
35	Consulta detalle de procesos de negocio.	4	1
36	Modificación de procesos de negocio.	4	1
37	Registro de alta o baja de procesos de negocio.	2	3
38	Consulta de alta o baja de procesos de negocio.	2	2
39	Modificación de baja o alta de procesos de negocio.	2	2
40	Registro de seguimiento de proceso de negocio.	3	3
41	Consulta de seguimiento de proceso de negocio.	3	2

42	Consulta detalle de seguimiento de proceso de negocio.	3	1
43	Modificación de seguimiento de proceso de negocio.	3	1
44	Generar reporte CMI.	4	3
45	Generar reporte indicadores clave de desempeño (Incidentes).	4	3
46	Generar reporte indicadores clave de desempeño (Planes de tratamiento).	4	3
47	Generar reporte indicadores clave de desempeño (Procesos de negocio).	4	3
48	Registro de usuario	4	3
49	Consulta de usuario	4	2
50	Consulta detalle de usuario	4	1
51	Modificación de usuario	4	1
52	Consulta de registro de actividades de usuarios.	3	3

Fuente: Elaboración propia.

5.6. Sprint Backlog del sistema Ecu@Risk

A partir de la lista del producto del sistema Ecu@Risk, se ha establecido que el desarrollo se lo realice en 6 Sprints de duración entre 10 y 13 días, con una semana extra para resolver tareas sesgadas de otros Sprint, se considera un desarrollo de 8 horas diarias por parte del equipo de trabajo. A continuación, se muestra la planeación de los Sprints para el desarrollo del sistema.

N. Sprint	Duración días
1	10
2	11
3	11
4	13
5	11
6	12
Extra	5
Total	73

Esta planificación tiene una duración aproximada de tres meses y medio laborales.

A continuación, se presenta el Sprint Block del sistema Ecu@Risk, con cada una de las tareas a realizarse en cada iteración y el tiempo estimado para el desarrollo de cada tarea.

Tabla 56:
Lista de tareas de elaboración del sistema Ecu@Risk.

Sprint Block			
SPRINT N	**Requerimiento**	**Tarea**	**Horas**
1	Creación del entorno de desarrollo para iniciar con el proyecto	Obtener las herramientas necesarias para la creación del entorno de desarrollo.	5
1		Creación del entorno de desarrollo.	5
1		Instalar y configurar el servidor web para la ejecución para la ejecución del sistema en el entorno.	4
1		Revisión del sistema del entorno de desarrollo para iniciar el proyecto.	3
1	Inicio de sesión y gestión de usuarios.	Creación de base de datos del sistema.	2
1		Creación de inicio de sesión de usuario.	8
1		Creación de pantalla de inicio para ADM.	3
1		Creación de pantalla de inicio para CSD.	3
1		Creación de pantalla de inicio para CRTI.	3
1		Creación de registro para usuarios.	4
1		Creación de consulta de usuarios.	3
1		Creación de consulta detalle de usuarios.	3
1		Creación de Modificación de usuarios.	2
1		Implementar el API de Google Authenticator.	12
1	Pruebas Sprint 1	Pruebas de Sprint 1.	16
2	Registro de activos de información.	Creación de formulario de registro de activos.	6
2		Generación automática de clave.	3
2		Cálculo y visualización de impacto de activo.	2
2		Valoración de activo.	3
2	Consulta de activos.	Creación de consulta de activos.	3
2		Creación de filtro de consulta: categoría de activo, código de activo, estado de activo.	2
2		Agregar ícono de "Ver detalle"	1
2		Agregar ícono de "Editar"	1

2	Consulta detalles de activos.	Creación de consulta de activo seleccionado.	2
2	Modificación de activos.	Cargar datos de activo seleccionado en formulario.	2
2	Registro de riesgos.	Creación de formulario de registro de riesgos.	5
2		Generación automática de clave.	3
2		Consulta y visualización de acuerdo a amenaza.	2
2		Ventana de elección de activos de información.	6
2		Filtración de información de ventana emergente por activos afectados.	3
2		Calificación de probabilidad.	2
2		Cálculo de riesgo absoluto.	4
2	Consulta de riesgos.	Creación de consulta de riesgos.	3
2		Creación de filtro de consulta: categoría de riesgo, código de riesgo, estado de riesgo.	2
2		Agregar ícono de "Ver detalle"	1
2		Agregar ícono de "Editar"	2
2	Consulta detalles de riesgo.	Creación de consulta de riesgo seleccionado.	2
2	Modificación de riesgo.	Cargar datos de riesgo seleccionado en formulario.	2
2	Pruebas Sprint 2	Pruebas de Sprint 2.	20
3	Relación de activo con riesgo.	Lista jerárquica de activos con relación a riesgos.	8
3		Creación de filtro de consulta: código de activo, código de riesgo.	4
3		Agregar ícono de "Definir plan de tratamiento".	1
3		Agregar ícono de "Ver detalle de plan de tratamiento".	1
3		Agregar ícono de "Editar plan de tratamiento".	1
3		Agregar ícono de Imprimir plan de tratamiento".	1
3	Registro de plan de tratamiento.	Creación de formulario de registro de plan de tratamiento.	5
3		Generación automática de clave.	3

3		Agregar plan de actividades.	5
3	Consulta de plan de tratamiento.	Creación de consulta de riesgos.	3
3		Creación de filtro de consulta: categoría de nombre, código de tratamiento, descripción de tratamiento.	2
3		Agregar ícono de "Ver detalle"	1
3		Agregar ícono de "Editar"	1
3		Agregar ícono de "Imprimir"	1
3		Agregar ícono de "Medición"	2
3	Consulta detalles de plan de tratamiento.	Creación de consulta de riesgo seleccionado.	2
3	Modificación de plan de tratamiento.	Cargar datos de riesgo seleccionado en formulario.	2
3	Medición de plan de tratamiento.	Creación de formulario de medición de plan de tratamiento.	6
3		Consulta de riesgo absoluto de cada activo.	3
3		Cálculo de riesgo residual.	5
3	Relación de activo, riesgo y tratamiento.	Lista jerárquica de activos con relación a riesgos y planes de tratamiento.	8
3		Creación de filtro de consulta: código de activo, código de riesgo, código de tratamiento.	3
3	Pruebas Sprint 3	Pruebas de Sprint 3	20
4	Registro de incidentes.	Creación de formulario de registro de incidentes.	4
4		Generación automática de clave.	3
4		Ventana de elección de activos de información.	4
4	Consulta de incidentes.	Creación de consulta de incidentes.	4
4		Creación de filtro de consulta: rango de fechas, categoría e incidente, subcategoría de incidente, código de activo.	3
4		Agregar ícono de "Ver detalle"	1
4		Agregar ícono de "Editar"	1
4	Consulta detalles de incidentes.	Creación de consulta de incidente seleccionado.	2
4	Modificación de incidentes.	Cargar datos de incidente seleccionado en formulario.	2

4	Registro de procesos de negocio.	Creación de formulario de registro de procesos de negocio.	5
4		Generación automática de clave.	3
4		Ventana de elección de activos de información.	3
4	Consulta de procesos de negocio.	Creación de consulta de procesos de negocio.	3
4		Creación de filtro de consulta: código de proceso de negocio, nombre, descripción de proceso de negocio, código de activo.	3
4		Agregar ícono de "Ver detalle"	1
4		Agregar ícono de "Editar"	1
4	Consulta detalles de procesos de negocio.	Creación de consulta de proceso de negocio seleccionado.	2
4	Modificación de procesos de negocio.	Cargar datos de proceso de negocio seleccionado en formulario.	2
4	Registro de seguimiento de procesos de negocio.	Creación de formulario de registro de seguimiento de procesos de negocio.	5
4		Creación de búsquedas: nombre de proceso de negocio, código de negocio.	5
4		Ventana de elección de incidentes.	4
4	Consulta de seguimiento de procesos de negocio.	Creación de consulta de seguimiento de procesos de negocio.	4
4		Creación de filtro de consulta: rango de fechas, código de seguimiento de proceso de negocio.	2
4		Agregar ícono de "Ver detalle"	1
4		Agregar ícono de "Editar"	1
4	Consulta detalles de seguimiento de procesos de negocio.	Creación de consulta de seguimiento de proceso de negocio seleccionado.	2
4	Modificación de seguimiento de procesos de negocio.	Cargar datos de seguimiento de proceso de negocio seleccionado en formulario.	2
4	Pruebas Sprint 4	Pruebas de Sprint 4	24
5	Reporte CMI.	Lista jerárquica de procesos de negocio relacionados con activos, riesgos y planes de tratamiento.	8
5		Creación de filtro de consulta: código de proceso de negocio, código de activo, código de riesgo, código de tratamiento.	3

5	Reporte indicador clave de desempeño (Incidentes).	Creación de lista jerárquica de incidentes relacionados con activos.	6
5		Creación de filtro de consulta: código de incidente, descripción de incidente, rango de fechas, categoría de incidente, subcategoría de incidente, código de activo.	3
5		Agregar ícono de "Imprimir reporte".	1
5	Reporte indicador clave de desempeño (Planes de tratamiento).	Creación de criterios de evaluación.	4
5		Creación de comparación de planes de tratamiento.	6
5		Creación de una lista jerárquica entre activos, riesgos y planes de tratamiento.	5
5		Agregar ícono de "Imprimir reporte".	1
5	Reporte indicador clave de desempeño (Procesos de negocio).	Creación de lista jerárquica de procesos de negocio relacionado con incidentes (seguimiento de procesos de negocio).	6
5		Creación de filtro de consulta: rango de fechas, proceso de negocio, incidentes.	3
5		Agregar ícono de "Imprimir reporte".	1
5	Actividades de usuario	Creación de lista de actividad y qué usuario lo realizó.	8
5	Imprimir	Imprimir reportes.	4
5		Imprimir planes de tratamiento.	4
5	Pruebas Sprint 5	Pruebas de Sprint 5	20
6	Registro de alta o baja de activos de información.	Creación de formulario para registro de baja o alta de activos.	5
6		Realizar búsqueda por código de activo.	4
6		Consultar información de activo.	2
6	Consulta de baja o alta de activo.	Creación de consulta de baja o alta de activos.	4
6		Creación de filtro de consulta: código de activo, fecha de modificación.	3
6	Modificación de baja o alta de activo.	Cargar datos de registro seleccionado en formulario.	2

6	Registro de alta o baja de riesgos.	Creación de formulario para registro de baja o alta de riesgos.	5
6		Realizar búsqueda por código de riesgo.	4
6		Consultar información de riesgo.	2
6	Consulta de baja o alta de riesgo.	Creación de consulta de baja o alta de riesgos.	4
6		Creación de filtro de consulta: código de riesgo, fecha de modificación.	3
6	Modificación de baja o alta de riesgo.	Cargar datos de registro seleccionado en formulario.	2
6	Registro de alta o baja de planes de tratamiento.	Creación de formulario para registro de baja o alta de planes de tratamiento.	5
6		Realizar búsqueda por código de plan de tratamiento.	4
6		Consultar información de plan de tratamiento.	2
6	Consulta de baja o alta de plan de tratamiento.	Creación de consulta de baja o alta de planes de tratamiento.	4
6		Creación de filtro de consulta: código de plan de tratamiento, fecha de modificación.	3
6	Modificación de baja o alta de plan de tratamiento.	Cargar datos de registro seleccionado en formulario.	2
6	Registro de alta o baja de procesos de negocio.	Creación de formulario para registro de baja o alta de procesos de negocio.	5
6		Realizar búsqueda por código de proceso de negocio.	4
6		Consultar información de riesgo.	2
6	Consulta de baja o alta de procesos de negocio.	Creación de consulta de baja o alta de proceso de negocio.	4
6		Creación de filtro de consulta: código de proceso de negocio, fecha de modificación.	3
6	Modificación de baja o alta de proceso de negocio.	Cargar datos de registro seleccionado en formulario.	2
6	Pruebas Sprint 6	Pruebas de Sprint 6	16
-	Semana de cierre	Completar tareas inconclusas	40

Fuente: Elaboración propia.

Conclusiones del capítulo 5

Los proyectos de desarrollo de software siempre necesitan de una metodología y una planificación para ser ejecutados. Para el desarrollo del sistema Ecu@Risk se opta por una metodología ágil, ya que proporciona todas las características que el sistema requiere para su desarrollo; por ejemplo, la rápida respuesta al cambio, el tiempo de elaboración, una planificación que puede adaptarse al equipo de desarrollo, etc. Las metodologías ágiles han dado excelentes resultados, clientes satisfechos y la garantía de ser aplicados en cualquier desarrollo de software; grandes empresas a nivel mundial como Facebook, PayPal, Apple, entre otras; realizan sus procesos de desarrollo mediante metodologías ágiles, llegando a ser empresas muy exitosas y un muy buen punto de referencia acerca de la implementación de metodologías ágiles en el desarrollo de proyectos en las empresas.

Las metodologías tradicionales tienen un enfoque diferente, ya que se centran más en la planificación y dan poco espacio en respuesta al cambio, que es un factor importante en el desarrollo de software en la actualidad, debido a la posibilidad de cambio que presenta un proyecto durante su ejecución; sin embargo, las metodologías tradicionales son muy utilizadas en la actualidad; por otro lado, las metodologías ágiles permiten el desarrollo de software de una manera más rápida en comparación con una tradicional.

La metodología Scrum es una metodología implementada por grandes empresas a nivel mundial, dando así una garantía de su funcionamiento y aplicación; esta metodología cuenta con una guía escrita en la cual se detalla cómo implementarla en un equipo de desarrollo de software.

Scrum define los roles de cada persona involucrada en el proyecto, los cuales son participantes activos que mantienen reuniones con el objetivo de dar a conocer todos los detalles del proyecto conforme avance el mismo, presentando evidencias que servirán como guía de planificación del desarrollo del proyecto, en este caso, el desarrollo del software informático Ecu@Risk.

Esta metodología es muy adaptable para cualquier grupo de trabajo; sin embargo, llegar a dominarla no es tarea sencilla como lo indican sus autores; pero, con la práctica, se puede ir poco a poco mejorando en su utilización, ya que esta metodología permite la retroalimentación de cada uno de los proyectos elaborados, y, en cada una de ellas se tendrá un constante aprendizaje.

Capítulo 6: Estudio económico

6.1. Introducción

Para iniciar el desarrollo del proyecto una parte muy importante es el presupuesto, la Gerencia de Proyectos Para Organizaciones de Desarrollo, PM4DEV por sus siglas en inglés (2009), define al presupuesto de un proyecto como la suma total de dinero ha sido asignado para el desarrollo del proyecto, con la finalidad de solventar todos los gastos del mismo, en un periodo de tiempo.

PM4DEV (2009) manifiesta que para que un proyecto se considere exitoso el alcance debe ser cumplido en su totalidad en el tiempo definido, dentro del presupuesto trazado y que el cliente esté satisfecho con la calidad del producto. Si se cumplen todos estos parámetros el proyecto ha sido un éxito total, en cambio, si uno de los parámetros falló el proyecto se considera un fracaso.

En este capítulo se analizará y desarrollará un estudio económico de todos los gastos que significará desarrollar el sistema Ecu@Risk, tomando en cuenta que la etapa de identificación de requerimientos y diseño del sistema ya han sido desarrolladas en capítulos anteriores.

6.2. Gestión de presupuesto de un proyecto.

El presupuesto, según (PM4DEV, 2009) debe ser controlado durante todo el ciclo de vida del proyecto, conjuntamente con los demás aspectos del proyecto; la gestión del presupuesto se divide en diferentes actividades y tareas que ayudarán en el manejo de costos del proyecto:

- Definir el presupuesto.
- Ejecutar el presupuesto.
- Controlar el presupuesto.
- Actualizar el presupuesto.

La gestión de presupuestos es necesaria para definir un plan de presupuestos con el que se solventará el desarrollo del proyecto, pero también es necesaria para controlar la inversión, es decir, que los gastos no sean mayores a los que se planificaron y que los pagos sean cumplidos conforme a lo acordado.

6.2.1. Presupuesto de un proyecto.

El director del proyecto es el encargado de la estimación del presupuesto requerido para cubrir todos los gastos para el desarrollo del mismo. El presupuesto debe ser muy detallado y también debe cubrir todos los aspectos del proyecto, ya sean estos: recursos humanos, materiales, insumos, en caso de ser necesario viajes, presupuesto para cubrir alguna eventualidad, etc. El director del proyecto también puede estimar el presupuesto, basándose en archivos e información acerca de anteriores proyectos, mediante el uso de herramientas especializadas o herramientas manuales como hojas de cálculo. (PM4DEV, 2009)

El director del proyecto decidirá cómo será la forma en que se efectuarán los pagos al equipo de desarrollo, en qué momento se realizarán las compras de los materiales necesarios, etc. Mientras se desarrolla el presupuesto del proyecto, pueden aparecer tareas y recursos adicionales, entre otros elementos. La lista del presupuesto del proyecto debe ser actualizada conjuntamente con la lista de planificación de tiempos y actividades. (PM4DEV, 2009)

Requerimiento de recursos

En este apartado la Gerencia de Proyectos Para Organizaciones en Desarrollo, PM4DEV (2009), indica que se debe determinar la cantidad de recursos se debe utilizar en el proyecto para cumplir con el desarrollo del mismo; el objetivo es obtener una lista de requerimientos de recursos el cual servirá para estimar el presupuesto y establecer los controles del mismo.

Una vez definido los recursos necesarios se procede a estimar los costos de cada uno de ellos, dando como resultado el presupuesto del proyecto. Este deberá ser presentado para su aprobación por parte de los interesados o las personas que vayan a financiarlo.

6.2.2. Ejecución del presupuesto

En este apartado PM4DEV (2009), indica que una vez aprobado el presupuesto, deben definirse las fases del proyecto en las que se medirá, monitoreará y controlará la gestión del presupuesto. Este plan debe ser comunicado a todas las personas que monitorearán y controlarán el presupuesto, con el fin de tomar decisiones de ser necesario con toda la información recolectada.

Poner en marcha el presupuesto es autorizar los gastos aprobados para el proyecto, como la contratación de personal, adquisición de equipos y materiales necesarios, etc. Esto se lleva a

cabo una vez sea aprobado el presupuesto y se dé inicio al cronograma del proyecto con sus actividades. (PM4DEV, 2009)

6.2.3. Control del presupuesto

Lo que se trata en este aparto es de monitorear y controlar al plan de presupuestos de acuerdo a lo planificado, y en caso de haber algún cambio se controla que solo los cambios apropiados sean incluidos en el plan de presupuesto inicial; el control es el proceso por el cual los costos del proyecto son debidamente identificados y pagados; en esta etapa las personas designadas son las encargadas de evaluar el presupuesto del proyecto. (PM4DEV, 2009)

En esta parte de la gestión del presupuesto, los reportes de las personas que lleven la parte financiera del proyecto son muy importantes, ya que estos documentos son una herramienta para dar seguimiento al presupuesto del proyecto y dan una clara idea de cómo sigues los gastos del plan del presupuesto definido. (PM4DEV, 2009)

6.2.4. Actualización del presupuesto

El presupuesto puede ser actualizado cuando existan cambios los cuales hayan sido aprobados por las personas que financian el proyecto; por ejemplo: el desarrollar una funcionalidad no contemplada dentro de la planificación. Este cambio es aprobado por el dueño del producto y requiere una replanificación en el cronograma y una actualización del presupuesto en donde se incluirá la nueva funcionalidad, en los reportes del nuevo presupuesto se incluirá también este cambio. Así mismo, si en los controles el presupuesto presenta algún inconveniente, se deben aplicar acciones correctivas las cuales serán discutidas por el director del proyecto y por el cliente. (PM4DEV, 2009)

PM4DEV (2009) manifiesta que los cambios en el presupuesto deben ser comunicados a todas las personas involucradas en su manejo, debido a que estas pueden estar realizando el control sobre actividades y planes cancelados. Finalmente, las lecciones aprendidas durante el desarrollo del presupuesto del proyecto deben ser aplicadas para corregir actividades del mismo proyecto o proyectos futuros, es muy importante siempre documentar cada paso en el proyecto.

6.3. Presupuesto del sistema Ecu@Risk

Para presupuestar el sistema Ecu@Risk deben considerarse algunos aspectos: el análisis de requerimientos del sistema, el diseño del sistema, la navegación y el diseño de la base de datos,

que ya han sido desarrollados a lo largo de los anteriores capítulos. El presupuesto del sistema se centrará en el desarrollo del mismo.

Recursos del proyecto

El software está dirigido a las empresas MPYMES; por lo tanto, en la elección de recursos para el proyecto se han buscado productos de desarrollo que tengan licencias de uso libre. El proyecto incluye el alquiler de un servicio de hosting para el alojamiento en la web del sistema, es un alquiler mensual.

Tabla 57:
Cotización de recursos para la elaboración del proyecto.

Recursos necesarios para el proyecto		
Recurso	**Descripción**	**Costo**
NetBeans IDE 8.1	Entorno de desarrollo integrado libre, implementado con lenguaje de programación Java.	Producto libre y sin restricciones de uso.
JavaServerFaces (JSF)	Framework para aplicaciones Java que están basadas en la web.	Producto libre y sin restricciones de uso.
PrimeFaces	Biblioteca para componentes de JavaServerFaces (JSF), facilita la creación de aplicaciones web.	Producto libre y sin restricciones de uso.
GlassFish Server 4.1	Servidor de aplicaciones.	Producto libre y sin restricciones de uso.
MySQL Workbench 6.3 CE	Herramienta visual de diseño de base de datos, la cual sirve para desarrollo de software, administración de base de datos, diseño de base de datos, creación y mantenimiento para el sistema de base de datos MySQL.	Sin costo para software GNU GPL.
VPS Hosting	Servidor conectado a internet. Proveedor: HostGator	$ 19,95/ al mes

Fuente: Elaboración propia.

El presupuesto de desarrollo del sistema ha sido cotizado en base al esfuerzo hora-hombre necesario para la elaboración de cada actividad.

Tabla 58:
Cotización de tareas para la elaboración del proyecto.

Desarrollo de requerimientos del sistema		
Requerimiento	**Horas**	**Costo $**
Creación del entorno de desarrollo para iniciar con el proyecto.	17	68,00
Inicio de sesión y gestión de usuarios.	43	172,00
Registro de activos de información.	14	56,00
Consulta de activos.	7	28,00
Consulta detalles de activos.	2	8,00
Modificación de activos.	2	8,00
Registro de riesgos.	25	100,00
Consulta de riesgos.	8	32,00
Consulta detalles de riesgos.	2	8,00
Modificación de riesgos.	2	8,00
Relación de activo con riesgo.	16	64,00
Registro de plan de tratamiento.	13	52,00
Consulta de plan se tratamiento.	10	40,00
Consulta detalles de plan de tratamiento.	2	8,00
Modificación de plan de tratamiento.	2	8,00
Medición de plan de tratamiento.	14	56,00
Relación de activo, riesgo y tratamiento.	11	44,00
Registro de incidentes.	11	44,00
Consulta de incidentes	9	36,00
Consulta detalles de incidentes.	2	8,00
Modificación de incidentes.	2	8,00
Registro de procesos de negocio.	11	44,00
Consulta de procesos de negocio.	8	32,00
Consulta detalle de procesos de negocio.	2	8,00
Modificación de procesos de negocio.	2	8,00
Registro de seguimiento de procesos de negocio.	14	56,00
Consulta de seguimiento de procesos de negocio.	8	32,00
Consulta detalles de seguimiento de procesos de negocio.	2	8,00
Modificación de seguimiento de procesos de negocio.	2	8,00
Reporte CMI.	11	44,00
Reporte indicador clave de desempeño (Incidentes).	10	40,00
Reporte de indicadores clave de desempeño (Planes de tratamiento).	16	64,00

Reporte de indicadores clave de desempeño (Procesos de negocio).	10	40,00
Actividades de usuario	8	32,00
Imprimir	8	32,00
Registro de alta o baja de activos de información.	11	44,00
Consulta de baja o alta de activo.	7	28,00
Modificación de baja o alta de activo.	2	8,00
Registro de alta o baja de riesgos.	11	44,00
Consulta de baja o alta de riesgo.	7	28,00
Modificación de baja o alta de riesgo.	2	8,00
Registro de alta o baja de planes de tratamiento.	11	44,00
Consulta de baja o alta de plan de tratamiento.	7	28,00
Modificación de baja o alta de plan de tratamiento.	2	8,00
Registro de alta o baja de procesos de negocio.	11	44,00
Consulta de baja o alta de procesos de negocio.	7	28,00
Modificación de baja o alta de proceso de negocio.	2	8,00
Pruebas Sprint 1	16	64,00
Pruebas Sprint 2	20	80,00
Pruebas Sprint 3	20	80,00
Pruebas Sprint 4	24	96,00
Pruebas Sprint 5	20	80,00
Pruebas Sprint 6	16	64,00
Total	**522**	**2088,00**

Fuente: Elaboración propia.

En el presupuesto del proyecto se incluye un monto de dinero que será utilizado para solventar los contratiempos que pueda sufrir el sistema, este monto es equivalente al 15% de la cotización inicial; este dinero será utilizado siempre y cuando el proyecto requiera solucionar problemas; si no es ocupado, se regresa la cantidad presupuestada.

El presupuesto del proyecto sin contemplar el monto de resolución de problemas del proyecto es:

Presupuesto	
Razón	**Costo $**
Desarrollo de requerimientos del sistema.	2.088,00
Alquiler de hosting (4 meses de desarrollo).	79,80
Total	2.167,80

El presupuesto final para el desarrollo del sistema Ecu@Risk es:

Presupuesto final	
Razón	**Costo $**
Desarrollo de requerimientos del sistema.	2.088,00
Alquiler de hosting (4 meses de desarrollo).	79,80
Riesgos del proyecto (15% del total del presupuesto).	325,17
Total	2.492,97

Plan de control y pagos

Los pagos y controles del presupuesto del proyecto serán en cada entrega del producto al cliente, distribuidos de la siguiente manera:

Plan de control y pago del proyecto		
Fase del proyecto	**Control**	**Pago $**
Inicio de proyecto	Inicio del proyecto	304,00
Sprint 1		
Sprint 2	Cierre de Sprint 2	328,00
Sprint 3	Cierre de Sprint 3	352,00
Sprint 4	Cierre de Sprint 4	388,00
Sprint 5	Cierre de Sprint 5	332,00
Sprint 6	Cierre de Sprint 6	384,00
	Total	2.088,00

El control del pago del alquiler del host se lo realizará cada mes, en la fecha que el proveedor del servicio lo solicite. Luego de concluido la etapa de desarrollo del sistema, se seguirá cumpliendo con el pago del host cada mes.

Conclusiones del capítulo 6

El presupuesto para el desarrollo, es una parte muy importante en la planificación de un proyecto, puesto que se trata, de la manera en cómo se solventarán los costos de los recursos, que son necesarios para la realización del proyecto; el director del proyecto es el encargado de elaborar este presupuesto, para la estimación de los costos, puede tomar en cuenta información histórica de otros proyectos elaborados por el equipo de trabajo. Este presupuesto es presentado al cliente que está interesado en realizar el proyecto, y él tiene la última palabra, puede aprobarlo o podría negociarlo, hasta conseguir un punto que beneficie a ambas partes.

El sistema Ecu@Risk es dirigido para empresas del sector MPYMES, y muchas de las veces estas empresas no cuentan con el capital para la inversión de un software de seguridad informática, o lo consideran un gasto innecesario, debido a que no están conscientes de la importancia de la seguridad en las labores de las empresas; por lo tanto, se ha buscado elaborar el sistema licencias de software libre, es decir, que no se tenga que pagar su uso, consiguiendo así un presupuesto razonable y asequible para que las empresas puedan invertir en un software que ayudará a gestionar sus activos de información.

Tener un presupuesto de respaldo para solventar problemas que se puedan suscitar durante el desarrollo del proyecto es un gran apoyo para el equipo de trabajo, debido a que el proyecto se tiene el respaldo económico para solucionar dichos problemas; estos problemas puede ser el resultado de la materialización de uno o varios riesgos en el desarrollo el proyecto, los riesgos siempre están presentes en la elaboración de los proyectos, este tema será tratado a profundidad en el siguiente capítulo.

El presupuesto del proyecto debe ser controlado periódicamente para asegurar que la cotización inicial no haya sufrido algún cambio a lo largo del desarrollo del proyecto, en caso que si tenga algún cambio, este debe ser hablado y aprobado con todas las personas que estén a cargo de las finanzas del proyecto, y todos estos cambios deben ser debidamente documentados, esto es muy importante porque la documentación se convierte en archivos históricos en los cuales pueden ser consultados para la elaboración de futuros proyectos.

Capítulo 7: Gestión de riesgos del proyecto

7.1. Introducción

Dentro de la gestión del proyecto se encuentra una parte muy importante como es la gestión de riesgos del proyecto, es decir, se trata de reducir o mitigar la probabilidad de impacto de algún evento que puede afectar el desarrollo normal de un proyecto. (Fernández Sanz & Bernad Silva, 2014)

Independientemente de la metodología de desarrollo que se utilice para la elaboración de un proyecto, siempre existirán riesgos, los cuales pueden afectar al proyecto en mayor o menor medida al desempeño y desarrollo del mismo, cuando los riesgos se llegan a materializar se obtienen problemas y retrasos en el desarrollo del proyecto, lo que conlleva a que se alteren planificaciones de tiempos y costes.

Controlar los riesgos permite que los proyectos se desarrollen con mayor agilidad, debido a que pueden solucionar rápidamente los inconvenientes y evitar retrasos en tiempos y ahorrar en costes; los autores Fernández Sanz y Bernad Silva (2014) definen a la gestión de riesgos como un proceso sistemático en el cual se identifica, se analiza y se planifica una respuesta hacia los riesgos que se presenten durante el ciclo de vida del proyecto, en donde el principal objetivo de la gestión de riesgos es el de minimizar la probabilidad y las consecuencias de que los eventos perjudiciales del proyecto.

7.2. Método de gestión de riesgos

La gestión de riesgos se ha convertido en una parte muy importante en el desarrollo de proyectos, varias normas han regulado y estandarizado los procesos de la gestión de riesgos como la guía de desarrollo de proyectos PMBOK. La norma mencionada anteriormente establece que las principales fases de la gestión de riesgos son: i) identificación de los riesgos que están presentes en el desarrollo del proyecto; ii) un análisis de los riesgos identificados, de manera cualitativa, cuantitativa o ambos; iii) un plan de respuestas hacia los riesgos que han sido identificados y evaluados; y finalmente iv) la fase de control y monitorización, cuya finalidad consiste en seguir la evolución de los riesgos que hayan sido tratados. (Fernández Sanz & Bernad Silva, 2014)

7.2.1. Plan de gestión de riesgos

Se elabora un plan de gestión en el cual se estable las directrices de cómo se gestionará los riesgos del proyecto en desarrollo. Como se mencionó anteriormente, este plan contiene la identificación de los riesgos, análisis, plan de respuesta a riesgos y seguimiento y control.

Para el autor Sebastián Rodríguez (2012), el factor humano juega un papel muy importante en la gestión, no solo como una fuente de generación de incertidumbre, sino como analista y facilitador de soluciones. En este punto, la experiencia del equipo de desarrollo del proyecto ayuda en alto grado a la elaboración del plan de gestión de riesgos.

7.2.2. Identificación de riesgos

En esta etapa se identifican los riesgos que pueden afectar al proyecto y se debe documentar todas sus características; es muy importante para el proyecto identificar los riesgos en etapas tempranas del desarrollo del proyecto, porque ya se contará con las medidas adecuadas. Sin embargo, la identificación de riesgos es un proceso iterativo, ya que algunos riesgos no contemplados pueden darse durante el desarrollo del proyecto. (Rodríguez, 2012)

Para la fase de identificación de los riesgos, los autores Fernández Sanz y Bernad Silva (2014) en su publicación señalan que existen listas en las cuales se colocan los factores de riesos más comunes que se pueden presentar en ell desarrollo de proyectos. El propósito de estas listas es el no ser exhaustivas y largas como lo son otros métodos de análisis de riesgos. El principal invonveniente de estas listas es que algunos riesgos poco comunes no sean considerados; sin embargo, según se desarrollen proyectos, el equipo de trabajo podrá seguir elaborando la lista de riesgos según las necesidades de cada uno.

7.2.3. Análisis cualitativo de los riesgos

Para realizar el análisis cualitativo de los riesgos identificados, la guía PMBOK de Project Management Institute (PMI) (2004) señala que “todos los riesgos tienen una probabilidad de que ocurran o no, y un determinado impacto si se llega a producir”. La guía proporciona parámetros tanto en probabilidad como en impacto. La valoración de la probabilidad es numérica una escala que va de 0 a 1; y la valorización del impacto también es numérica dependiendo de las diferentes categorías (muy bajo, bajo, moderado, alto y muy alto). A continuación, se presenta una tabla donde la guía PMBOK (2004) evalúa los objetivos principales del proyecto.

Tabla 59:
Matriz de escalas de impacto.

Condiciones definidas de la escala de impactos de un riesgo en los objetivos principales					
Objetivo del proyecto	Escalas relativas o numéricas				
	Muy bajo/0.05	Bajo/0.1	Moderado /0.2	Alto/0.4	Muy Alto/0.8
Coste	Incremento insignificante en el coste	Incremento del coste < 10%	Incremento del coste 10 - 20%	Incremento del coste 20 - 40%	Incremento del coste > 40%
Tiempo	Incremento insignificante en el tiempo	Incremento del tiempo < 5%	Incremento del tiempo 5 - 10%	Incremento del tiempo 10 - 20%	Incremento del coste > 20%
Alcance	Reducción del alcance insignificante	Área menores del alcance afectadas	Áreas considerables de alcance afectadas	Alcance reducido sensibemente	Alcance reducido drásticamente
Calidad	Degradación de la calidad insignificante	Degradación de la calidad poco perceptible	Degradación de la calidad requiere aprobación	Degradación de la calidad poco aceptable	Degradación de la calidad poco aceptable

Fuente: (Project Management Institute, 2004).

7.2.4. Plan de respuesta frente a riesgos

Una vez concluido el análisis de los riesgos que han sido identificados, se debe determinar cómo se debe proceder ante las amenazas. La guía PMBOK (2004) sugiere elaborar un plan de respuesta frente a los riesgos. Las respuestas pueden estar planificadas de acuerdo a la necesidad del proyecto frente al riesgo identificado. En la guía se proporciona posibles formas de actuar frente a los riesgos:

- Supresión del riesgo: esta acción se refiere a los cambios que se tiene que realizar en el plan del proyecto para anular los riesgos y sus consecuencias.
- Transferencia del riesgo: esta acción se refiere a que la gestión del riesgo es responsabilidad de otra organización. Transerir el riesgo no anula al riesgo en si ni sus consecuencias, solamente se está transfiriendo a otro la responsabilidad.
- Mitigación del riesgo: esta acción se refiere a reducir la probabilidad y consecuencias si el riesgo llega a materializarse, lo que se intenta en esta acción es reducir el riesgo hasta niveles que sean factiles o aceptables.
- Aceptar el riesgo: esta acción se da cuando no se decide cambiar de ninguna manera el plan del proyecto, o no se ha podido hallar una solución para dicho riesgo.

El plan de respuestas ante riesgos es muy importante dentro la gestión de riesgos, sin embargo, el mismo debe ser realista y debe adaptarse a la realidad del proyecto que se está desarrollando, tanto en cuestiones económicas, de tiempo, de alcance y calidad del proucto final.

7.2.5. Seguimiento y control de riesgos

La fase final es el seguimiento y control, la gestión de riesgos es un proceso dinámico, lo que significa que siempre se debe estar en constante revisión de los riesgos en el proyecto, sea que estos se hayan materializado o no, debido a que se pudieron presentar nuevas amenazas durante el ciclo de vida del proyecto, lo que obliga a los encargados a dar un seguimiento y no abandonarlo luego de la planificación de la gestión de riesgos.

El seguimiento de los riesgos permite evaluar si el plan de respuestas desarrollado fue efectivo para controlar los riesgos que se hayan presentado; estos controles permitirán decidir si es necesario tomar medidas de emergencia, si se requiere reformular el plan de respuesta, etc. (Rodríguez, 2012)

Sebastián Rodriguez (2012) manifiesta que es necesario la comunicación de todas las partes interesadas en el proyecto para comprobar los niveles de los riesgos, tomando en cuenta los siguientes puntos:

- Se muestran indicios de aparición de riesgos.
- Las repuestas de los riesgos han sido aplicadas como se lo ha planificado.
- Las respuestas que han sido planificadas para los riesgos han sido efectivas, o deben sustituirse por otras.
- El riesgo que afecta al proyecto ha cambiado desde el último análisis efectuado.
- Se siguen las políticas y procedimientos adecuadas.
- Se han presentado riesgos que no hayan sido identificados.

7.3. Gestión de riesgos en metodologías ágiles

Sin importar la metodología de desarrollo del proyecto, sea una metodología ágil o sea una metodología tradicional, los riesgos y amenazas siempre estarán presentes y pueden afectar de mayor o menor medida al normal desarrollo del proyecto. Debe contarse con un plan de gestión de riesgos, el cual garantice el normal desarrollo del proyecto, cubriendo todos los inconvenientes posibles que se pueden suscitar.

Se piensa que la gestión de riesgos en las metodologías ágiles está implícito debido a su carácter de iterativo, es decir, que a los riesgos se los están tratando durante todo el ciclo de vida del proyecto, dependiendo de cómo se manejen los problemas en cada metodología. Sin embargo, se sugiere elaborar un plan de gestión de riesgos estructurado, explícito y predictivo, el cual ayudará a estar preparado o solventar cualquier problema al equipo de trabajo. (Amaya Balaguera, 2013)

Se plantea desarrollar el sistema Ecu@Risk mediante la metodología ágil Scrum. Para Amaya Balaguera (2013) los riesgos se están tratando iterativamente en cada reunión de Scrum Diario, en la reunión de preparación del Sprint, en las reuniones de revisón y las reuniones de retrospectiva, en donde se pueden tratar los problemas que surjan en el transcurso del proyecto, como se explicó en capítulos anteriores. Sin embargo, se recalca que todos los riesgos deben ser gestionados sean estos internos o externos al proyecto.

Para el desarrollo del sistema Ecu@Risk se elaborará un plan de gestión de riesgos el cual tendrá la estructura propuesta por la guía PMBOK, el plan será adaptado a la metodoloía desarrollo del proyecto, la metoología ágil Scrum, el plan tendrá la identificación de los riesgos del proyecto, el análisis de los riesgos, el plan de respuestas al riesgo y finalmente un modelo de seguimiento en caso de riesgos que se hayan materializado.

7.4. Plan de riesgos para la elaboración del sistema Ecu@Risk

Para la etapa de identificación, se utilizó los factores de riesgo en proyectos de desarrollo de software divididos en las cateegorías de personas, procesos de desarrollo, producto y tecnología, los mismos que fueron descritos por la autora Ramírez Zuluaga (2011). Para el desarrollo del sistema Ecu@Risk se formó una lista de trece factores de riesgo que estarán presentes en este proyecto, cómo se lo mencionó anteriormente, esta lista puede crecer conforme se avance con el desarrollo del proyecto ya que se pueden presentar otros riesgos que no fueron contemplados, se recomienda añadir estos riesgos a esta lista para futuros desarrollos.

Se realiza un análisis cualitativo de cómo el riesgo afecta a los parámetros de tiempo, coste, alcance y calidad del proyecto, se toma en cuenta el factor de probabilidad de que el riesgo llegue a ocurrir y en base a eso, se clasifica si el riesgo es alto, medio o bajo para el proyecto.

Para el plan de respuestas a los riesgo, se clasifica a los riesgos de mayor a menor según su calificación en la etapa anterior y se elabora las respuestas necesarias para los riesgos, también se especifíca quién va a ser el responsable o responsables de ejecutar las respuestas.

La etapa de monitorización y control no solo se lleva a cabo cuando el riesgo se materialice, más bien, es una proceso que siempre se debe estar en constante ejecución, es decir, monitorizar que no se presenten los síntomas de aparición del riesgo. En caso de que el riesgo se de en el proyecto, se aplican los planes de respuesta y se ejecuta el control del riesgo, es decir, cómo evoluciona a o largo del proyecto, si el plan de respuesta fue suficiente, es necesario tomar nuevas medidas, etc. Todo el proceso de monitorización y control se debe realizar por parte de la dirección del proyecto, dejando constancia de este proceso a través de informes y documentación, misma que servirá para el desarrollo de futuros proyectos.

Los resultados de la identificación, análisis y planes de respuesta se los presenta, por medio de las siguientes tablas.

Identificación y análisis cualitativo de factores de riesgos							
Código de Riesgo	**Descripción del Riesgo**	**Causa**	**Estimación de Probabilidad**	**Objetivo Afectado**	**Estimación de Impacto**	**Probabilidad X Impacto**	**Tipo de Riesgo**
R001	**Planificación del proyecto demasiado optimista:** Elaborar una planificación sin tomar en consideración los retrasos que puede llegar tener el proyecto o menospreciando el alcance del mismo, puede hacer que las actividades sean cumplidas a medias, provocando presión dentro del equipo de trabajo, afectando su moral y su productividad.	Equipos de trabajo con falta de experiencia en la planificación de proyectos.	0,4	Alcance	0,2	0,08	Alto
				Tiempo	0,4	0,16	
				Coste	0,2	0,08	
				Calidad	0,2	0,08	
				Total Probabilidad X Impacto		**0,4**	
R002	**Diseño inadecuado del sistema:** los diseños del sistema no cumplen los requerimientos del software y no llenan las expectativas de los clientes conforme a lo acordado.	Requerimientos no levantados correctamente.	0,2	Alcance	0,4	0,08	Alto
				Tiempo	0,4	0,08	
				Coste	0,4	0,08	
				Calidad	0,4	0,08	
				Total Probabilidad X Impacto		**0,32**	
R003	**Pruebas de software insuficientes, comprometiendo la calidad:** las pruebas que se realizan al sistema no garantizan su calidad, debido a que se encuentran diferentes errores y problemas con el software y los clientes no están satisfechos con la calidad del producto entregado.	La planificación de pruebas que se realizan al sistema, no son exhaustivas.	0,6	Alcance	0,1	0,06	Alto
				Tiempo	0,4	0,24	
				Coste	0,1	0,06	
				Calidad	0,2	0,12	
				Total Probabilidad X Impacto		**0,48**	
R004	**Planificación insuficiente:** el proyecto no ha sido planificado de acuerdo al alcance y complejidad de cada parte del sistema, provocando un déficit en los tiempos de las actividades.	Equipos de trabajo con falta de experiencia en la planificación de proyectos.	0,2	Alcance	0,2	0,04	Medio
				Tiempo	0,4	0,08	
				Coste	0,4	0,08	
				Calidad	0,2	0,04	

				Total Probabilidad X Impacto		**0,24**	
R005	**Insuficientes controles por parte de la dirección del proyecto:** poco control de los dirigentes del proyecto para descubrir síntomas de posibles contratiempos, lo que ocasiona que el proyecto empiece a presentar problemas.	Poca planificación de controles del proyecto, poco compromiso en el proyecto por parte de la dirección.	0,3	Alcance	0,05	0,015	Medio
				Tiempo	0,2	0,06	
				Coste	0,4	0,12	
				Calidad	0,2	0,06	
				Total Probabilidad X Impacto		**0,255**	
R006	**Cambios significantes de requisitos del sistema:** cambios en los requisitos levantados, mismos que se encuentran terminados o en desarrollo, dichos cambios puede que afecten a parte o a la totalidad de algún componente del sistema.	Los clientes no están seguros ni claros de lo que realmente desean en el sistema.	0,1	Alcance	0,2	0,02	Bajo
				Tiempo	0,8	0,08	
				Coste	0,8	0,08	
				Calidad	0,1	0,01	
				Total Probabilidad X Impacto		**0,19**	
R007	**Desarrolladores añaden características no especificadas en los requisitos:** los programadores se desvían de los requisitos iniciales y añaden características innecesarias en el sistema, lo que puede ocasionar el retraso en el desarrollo de las demás tareas y que los clientes estén insatisfechos con el resultado porque no es el requerido.	Incorrecta redacción de las tareas asignadas a los programadores y falta de revisión de la dirección del proyecto.	0,2	Alcance	0,1	0,02	Bajo
				Tiempo	0,2	0,04	
				Coste	0,05	0,01	
				Calidad	0,2	0,04	
				Total Probabilidad X Impacto		**0,11**	
R008	**Corromper el alcance del sistema:** el añadir o modificar significativamente los requisitos del proyecto de manera constante sin importar en qué fase del proyecto se encuentre, causa problemas en el desarrollo del proyecto.	Aceptar todos los cambios por parte de los directivos y no negociar con el cliente.	0,15	Alcance	0,8	0,12	Medio
				Tiempo	0,4	0,06	
				Coste	0,4	0,06	
				Calidad	0,2	0,03	
				Total Probabilidad X Impacto		**0,27**	

R009	**Sobrevalorar el ahorro de tiempo al utilizar nuevas herramientas o métodos:** el utilizar una nueva herramienta tecnológica o un método nuevo de desarrollo, puede llevar un tiempo para aprender a usarlo de forma correcta.	Actualizar las herramientas o métodos de desarrollo.	0,2	Alcance	0,05	0,01	Medio
				Tiempo	0,4	0,08	
				Coste	0,4	0,08	
				Calidad	0,2	0,04	
				Total Probabilidad X Impacto		**0,21**	
R010	**Personal no adecuado en el proyecto:** personas que no deben estar en el proyecto, tienen falta de conocimientos, experiencia, no están comprometidos con el proyecto, son problemáticas, etc.	Contratación del personal sin pruebas y entrevistas adecuadas.	0,4	Alcance	0,1	0,04	Alto
				Tiempo	0,2	0,08	
				Coste	0,4	0,16	
				Calidad	0,2	0,08	
				Total Probabilidad X Impacto		**0,36**	
R011	**Baja productividad del equipo de desarrollo:** no se cumplen las metas propuestas en la planificación, se retrasan mucho las tareas, etc.	La motivación en el equipo no es suficiente o no es adecuada, el ambiente de trabajo no es el propicio para el equipo.	0,45	Alcance	0,1	0,045	Alto
				Tiempo	0,4	0,18	
				Coste	0,4	0,18	
				Calidad	0,2	0,09	
				Total Probabilidad X Impacto		**0,495**	
R012	**Diferencias entre el equipo de trabajo:** Los problemas entre el personal se convierte en una carga muy pesada en el desarrollo del proyecto.	Personal con problemas de comunicación, empleados problemáticos, equipo que no se pone de acuerdo, etc.	0,5	Alcance	0,1	0,05	Alto
				Tiempo	0,4	0,2	
				Coste	0,2	0,1	
				Calidad	0,2	0,1	
				Total Probabilidad X Impacto		**0,45**	

R013	**Problemas con los clientes:** roces constantes con los clientes, al no ponerse de acuerdo, lo que causa problemas muy graves en el desarrollo del proyecto.	Mala relación de ambas partes, mala comunicación, requerimientos entendidos y desarrollados pobremente, mal funcionamiento del sistema, etc.	0,3	Alcance	0,4	0,12	Alto
				Tiempo	0,2	0,06	
				Coste	0,4	0,12	
				Calidad	0,2	0,06	
				Total Probabilidad X Impacto		**0,36**	

Roles del Plan de Riesgos
Scrum Master
Product Owner
Development Team
Gerente

Plan de respuestas						
Código de Riesgo	**Descripción del Riesgo**	**Probabilidad X Impacto Total**	**Tipo de Riesgo**	**Respuestas Planificadas**	**Responsable**	**Control y Monitorización**
R011	**Baja productividad del equipo de desarrollo:** no se cumplen las metas propuestas en la planificación, se retrasan mucho las tareas, etc.	0,495	Alto	Realizar una reunión con todos los miembros del equipo en la que todos puedan dar a conocer sus opiniones a cerca del proyecto, lo que les aqueja, si es algo específico lo que les molesta, etc. Es decir en que los miembros del equipo puedan expresarse.	Scrum Master	Se debe monitorizar y controlar este riesgo en cada Sprint, es recomendable al menor síntoma de aparición de este riesgo activar los planes de respuesta, debido a que no se debe permitir que la baja productividad crezca durante el desarrollo del proyecto.
				Identificar el cuello de botella, es decir, hacer un análisis de cómo es la producción de cada miembro del equipo, evaluar sus tareas entregadas y aprobadas, cuántas no han sido aprobadas, etc.		

				Motivar siempre al equipo de trabajo, comunicación constante, recalcar la importancia del proyecto, cada miembro debe sentirse parte importante del proyecto.		
R003	**Pruebas de software insuficientes, comprometiendo la calidad:** las pruebas que se realizan al sistema no garantizan su calidad, debido a que se encuentran diferentes errores y problemas con el software y los clientes no están satisfechos con la calidad del producto entregado.	0,48	Alto	Realizar pruebas exahustivas de elementos funcionales, no funcionales, estructurales, pruebas de regresión y re-pruebas. Asignar una persona que realice las pruebas necesarias para que encuentren problemas y fallas en el software antes de entregar a los clientes y que los desarrolladores los corrijan. Desarrollar pruebas automatizadas con software del mercado, que pueda ahorrar tiempo a la persona encargada de hacer las pruebas y aumentar su productividad en el proyecto.	Scrum Master	Se debe monitorizar y controlar este riesgo en cada entrega a los clientes, si el riesgo estalla, es decir, los clientes encuentran muchos errores en el sistema, se debe poner en marcha el o los planes de respuesta.
R012	**Diferencias entre el equipo de trabajo:** Los problemas entre el personal se convierte en una carga muy pesada en el desarrollo del proyecto.	0,45	Alto	Reuniones con el equipo de trabajo en donde se traten temas de compañerismo y tratar de saber cuáles son las causas de las diferencias entre las personas y tratar de llegar a solucionar estos problemas, para crear un ambiente mejor de trabajo para todos. Si la situación persiste, separar del grupo a el o las personas que sean dañinas para el desarrollo del proyecto.	Scrum Master / Development Team	Cada persona es diferente, lo cual significa que no se sabrá cómo será su adaptación para el trabajo en equipo, se debe siempre estar pendiente de cómo está el grupo de trabajo y si el riesgo se llega a dar, aplicar los planes, este riesgo siempre debe ser monitorizado y controlado desde el inicio hasta el fin del proyecto.
R001	**Planificación del proyecto demasiado optimista:** Elaborar una planificación sin	0,4	Alto	Replanificación de inmediato del proyecto tomando en consideración los factores que hayan surgio en el	Product Owner / Scrum Master /	La monitorizacióno y control debe ser constante desde el inicio del proyecto, el plan de respuesta

	tomar en consideración los retrasos que puede llegar tener el proyecto o menospreciando el alcance del mismo, puede hacer que las actividades sean cumplidas a medias, provocando presión dentro del equipo de trabajo, afectando su moral y su productividad.			desarrollo (retreasos, ritmo el equipo, etc.) Todo el equipo de desarrollo debe estar involucrado.	Development Team	ha este riesgo se debe activar al mínimo síntoma de presentarse, debido a que el cliente debe estar enterado del tiempo real que su producto tardará y costará.
R013	**Problemas con los clientes:** roces constantes con los cientes, al no ponerse de acuerdo, lo que causa problemas muy graves en el desarrollo del proyecto.	0,36	Alto	Reunión entre los clientes y la direccióno del proyecto, identificar el punto de discrepacia, tratar temas acerca de qué piensa el cliente sobre el trabajo del equipo, ofrecer soluciones que sean del agrado del cliente, comunicación continua de ambas partes, y compromiso total en el proyecto.	Product Owner / Scrum Master	Este riesgo debe ser monitorizado y controlado en cada reunión con el cliente, en cada entrega, en cada participación, es decir, constantemente se debe medir la satisfacción del cliente, para evitar que este riesgo llegue a ocurrir, y en caso de que se presente un síntoma del riesgo se debe poner en marcha el plan de respuesta.
R010	**Personal no adecuado en el proyecto:** personas que no deben estar en el proyecto, tienen falta de conocimientos, experiencia, no están comprometidos con el proyecto, son problemáticas, etc.	0,36	Alto	Identificar al personal que no está siendo un aporte para el proyecto, llamarlos a reuniones por separado y tratar su problema, llamando al compromiso para el proyecto. Separar del personal a las personas que no son aecuadas para el proyecto.	Scrum Master	Se debe estar en constante monitorización y control de este riesgo, desde el principio del proyecto, hasta la finalización.
R002	**Diseño inadecuado del sistema:** los diseños del sistema no cumplen los	0,32	Alto	Realizar una reunión de carácter urgente con el cliente, y repasar los requerimientos del sistema, identificar	Product Owner / Scrum Master /	Este riesgo se debe monitorizar y controlar en todas las entregas del producto al cliente, y al presentar

	requerimientos del software y no llenan las espectativas de los clientes conforme a lo acordado.			los requerimientos mal diseñados o que no concuerdan con la petición del cliente; entrar en una etapa de rediseño de los componentes afectados y presentarlos para aprobación del cliente.	Development Team	un síntoma de aparición de este riesgo, ejecutar el plan e respuesta.
R008	**Corromper el alcance del sistema:** el añadir o modificar significativamente los requisitos del proyecto de manera constante sin importar en qué fase del proyecto se encuentre, causa problemas en el desarrollo del proyecto.	0,27	Medio	Realizar reuniones con el cliente para negociar cada cambio significante que tenga en mente para el sistema, se debe negociar estos cambios, es decir, hacerle ver al cliente lo que significará el cambio en términos de tiempo, costo y alcance.	Product Owner / Scrum Master	Se monitoriza y controla este riesgo en cada cambio del cliente, se debe analizar cómo afectará el desarrollo del proyecto; si se detecta que afecta de manera negativa se pone en marcha el plan de respuesta.
R005	**Insuficientes controles por parte de la dirección del proyecto:** poco control de los dirigentes del proyecto para descubrir sintomas de posibles contratiempos, lo que ocaciona que el proyecto empiece a presentar problemas.	0,255	Medio	Reunión con la directiva del proyecto encagada de los controles del mismo (Scrum Master, Product Owner), solicitar compromiso total con el proyecto, y los controles de tiempo y presupuesto. Si los problemas persisten con la directiva aplicar sansiones económicas, o separarlos del equipo de trabajo.	Gerente	Se monitoriza y controla este riesgo desde el inicio del proyecto, es decir, es de acción continua, se necesitan informes al día del proyecto del progreso del proyecto por parte de la dirección del mismo, con el fin de constatar que no exista ningún inconveniente en el desarrollo del mismo, si se detecta un síntoma de este riesgo, de inmediato poner en marcha el plan de respuesta.

R004	**Planificación insuficiente:** el proyecto no ha sido planificado de acuerdo al alcance y complejidad de cada parte del sistema, provocando un déficit en los tiempos de las actividades.	0,24	Medio	Replanificación de inmediato del proyecto tomando en consideración los factores que hayan surgio en el desarrollo (retreasos, ritmo el equipo, etc.) Todo el equipo de desarrollo debe estar involucrado.	Product Owner / Scrum Master	La monitorización y control debe ser constante desde el inicio del proyecto, el plan de respuesta ha este riesgo se debe activar al mínimo síntoma de presentarse, debido a que el cliente debe estar enterado del tiempo real que su producto tardará y costará.
R009	**Sobrevalorar el ahorro de tiempo al utilizar nuevas herramientas o métodos:** el utilizar una nueva herramienta tecnológica o un método nuevo de desarrollo, puede llevar un tiempo para aprender a usarlo de forma correcta.	0,2	Medio	Proveer al equipo de desarrollo del proyecoto cursos y material con el cual pueden aprender más rápido el funcionamiento de la herramienta o método nuevo integrado en el equipo. Los cursos pueden ser en línea o presenciales, se requiere de realizarlos en horario fuera de horario de trabajo.	Scrum Master / Development Team	Este riesgo debe ser monitorizado y controlado desde el inicio del proyecto en acción continua, y al presentarse problemas por parte de los desarrolladores como retreasos por falta de conocimiento de la herramienta o método utilizado se debe poner en marcha el plan de respuesta.
R006	**Cambios significantes de requisitos del sistema:** cambios en los requisitos levantados, mismos que se encuentran terminados o en desarrollo, dichos cambios puede que afecten a parte o a la totalidad de algún componente del sistema.	0,19	Bajo	Realizar reuniones con el cliente para negociar cada cambio significante que tenga en mente para el sistema, se debe negociar estos cambios, es decir, hacerle ver al cliente lo que significará el cambio en términos de tiempo, costo y alcance.	Product Owner / Scrum Master	Se monitoriza y controla este riesgo en cada cambio del cliente, se debe analizar cómo afectará el desarrollo del proyecto; si se detecta que afecta de manera negativa se pone en marcha el plan de respuesta.

R007	**Desarrolladores añaden características no especificadas en los requisitos:** los programadores se desvían de los requisitos iniciales y añaden características innecesarias en el sistema, lo que puede ocasionar el retraso en el desarrollo de las demás tareas y que los clientes estén insatisfechos con el resultado porque no es el requerido.	0,11	Bajo	Realizar una reunión con los desarrolladores del sistema e indicar los requisitos y especificaciones que han sido entregadas por los clientes, indicar también que se deben apega estrictamente a las tareas especificadas por la dirección del proyecto.	Scrum Master/ Development Team	Este riesgo debe ser monitorizado y controlado en cada entrega de las actividades por parte de los programadores, en donde se revisarán que esté de acuerdo con los requisitos dados por el cliente. Si se presentan síntomas de aparición este riesgo en el proyecto, se debe poner en marcha de inmediato el plan de respuesta.

Conclusiones del capítulo 7

Los riesgos nacen de la incertidumbre y se encuentran latentes en todos los proyectos, sin importar la metodología de desarrollo que se utilice. Esto significa que siempre se debe gestionar los riesgos en los proyectos, ya que gracias a esto, el equipo está preparado y sabe qué hacer ante un problema que se presente, garantizando así que el desarrollo del proyecto no se vea perjudicado y se puede salir adelante.

A pesar que la metodología de desarrollo del sistema Ecu@Risk es una metodología ágil, se implementó un análisis y planificación dado por una metodología de desarrollo tradicional como es la guía de PMBOK; estas directrices son factibles de implementar debido a que la guía evalúa los mismos parámetros con los que se construye y maneja un este proyecto que se desarrollará con una metodología ágil. Se cree que los riesgos son tratados de forma implícita por cada metodología ágil debido a su carácter iterativo, sin embargo, se recomienda elaborar un plan que no solo trate los riesgos internos del proyecto sino también los externos.

El plan de gestión de riesgos del proyecto se debe ajustar a la realidad económica y política del equipo de trabajo, debido a que serán las medidas que se tomarán para solventar los riesgos y, elaborar un plan fantasioso y poco realista perjudicaría al proyecto en lugar de ayudarlo.

Los riesgos siempre deben estar en constante monitorización. No se debe abandonar el plan de gestión de riesgos al inicio del proyecto, sino debe ser un proceso constante e iterativo en busca del menor síntoma de la aparición de cualquier riesgo. Si un riesgo llega a materializarse se debe seguir un control del mismo, es decir, después de aplicar el plan de respuesta, se debe evaluar si los procedimientos del plan fueron eficientes para solucioonar el problema o si se debe tomar nuevas medidas, etc. Toda esta información debe ser documentada para así poder seguir actualizando el plan de gestión de riesgos el cuál servirá para futuros proyectos.

La lista de factores de riesgo puede ser actualizada conforme se desarrolla el proyecto, debido a que el equipo puede detectar otro riesgo que no haya sido considerado en el plan. Inmediatamente este deberá ser actualizado y deberán tomarse las medidas necesarias para tratar al nuevo riesgo, nuevamente la monitorización y control es parte fundamental del proyecto, en cuanto a los riesgos se trata.

Capítulo 8: Desarrollo de prototipo

8.1. Introducción

En este capítulo se presentará el desarrollo de una parte del sistema de gestión de seguridad de la información Ecu@Risk, la cual se centra en mostrar la funcionalidad del sistema en gestión de usuarios, gestión de activos, riesgos y planes de tratamiento.

En este apartado se detallarán las funciones del prototipo, al igual de cómo se realizan los cálculos de los riesgos, cuáles son los procedimientos clave, etc. Para tener una idea clara de cómo será la implementación del sistema.

8.2. Prototipo del sistema Ecu@Risk

Una vez concluido las etapas de levantamiento de requerimientos y diseño del sistema. se desarrolló un prototipo, el cual se compone de: inicio de sesión, gestión de usuarios, gestión de activos, gestión de riesgos, y gestión de tratamientos.

El prototipo ha sido desarrollado en el localhost, utilizando NetBeans IDE 8.1 como entorno de desarrollo, JavaSererFaces como framework, GlassFish Server 4.1 como servidor de aplicaciones y MySQL Workbench 6.3 CE como gestor de base de datos.

8.2.1. Inicio de sesión

El sistema muestra una interfaz de inicio de sesión, en la cual, solo pueden acceder los usuarios que hayan sido registrados como administrador o coordinador se seguridad designado.

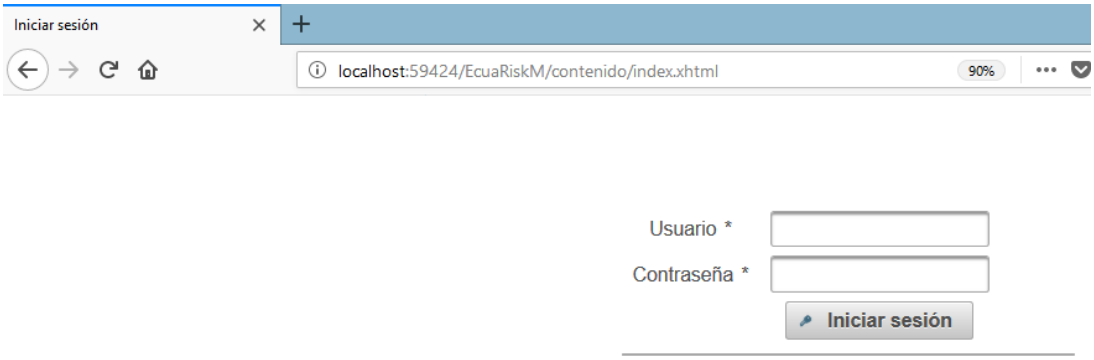

Ilustración 173: Inicio de sesión.
Fuente: Elaboración propia.

8.2.2. Gestión de usuarios

La gestión de usuarios desarrollado en el prototipo tiene que ver con la creación, edición y listado de usuarios. Cada usuario tiene su propia interfaz de trabajo, a la gestión de usuarios únicamente tienen acceso los administradores del sistema.

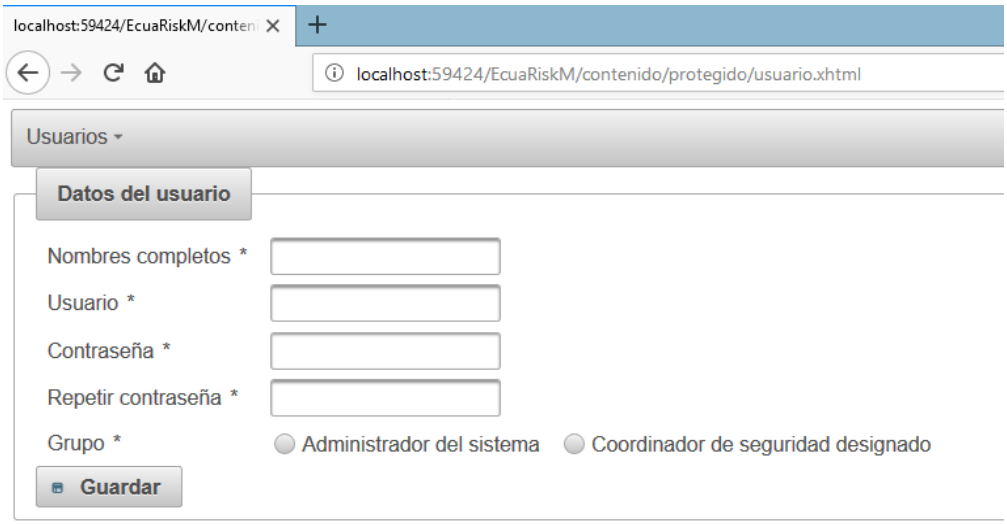

Ilustración 174: Creación o Edición de usuario.
Fuente: Elaboración propia.

Ilustración 175: Listado de usuarios.
Fuente: Elaboración propia.

8.2.3. Gestión de activos

El usuario que tiene acceso a la gestión de activos, es el usuario coordinador de seguridad designado, aquí el usuario podrá crear activos de información, listarlos y modificarlos.

En la creación o edición de activos de información, el usuario ingresará los datos que el sistema solicite, si se ingresa un activo el sistema se genera un código automático; cuando se ingrese o modifique la valoración en confidencialidad, integridad y disponibilidad, el sistema automáticamente calculará la valoración total y cualitativa, así como también el impacto de las dimensiones del activo.

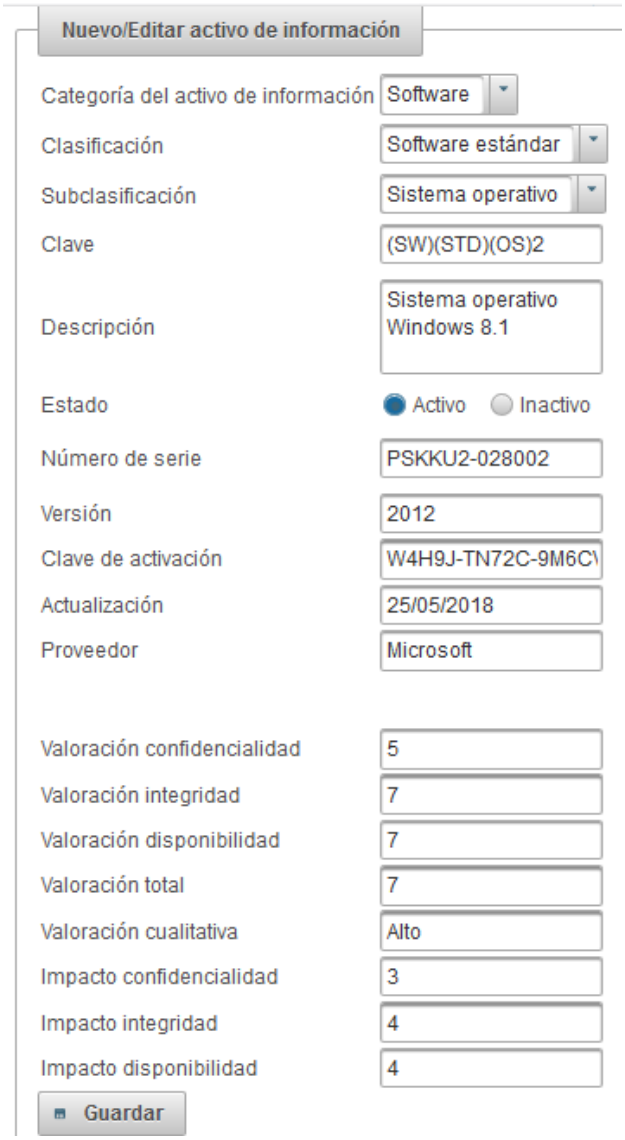

Ilustración 176: Registro o edición de un activo de información.
Fuente: Elaboración propia.

El sistema lista todos los activos que hayan sido registrados y ofrece las opciones de "Editar" su información y consultar el "Detalle" de los registros.

Ilustración 177: Lista de activos registrados.
Fuente: Elaboración propia.

8.2.4. Gestión de riesgos y tratamientos

La gestión de riesgos y tratamientos es manejada por el usuario coordinador de seguridad designado, es el encargado de registrar o editar los riesgos del sistema, así como los planes de tratamiento.

Para la gestión de riesgos, el usuario debe escoger qué tipo de amenaza representa el riesgo a registrar y el sistema automáticamente muestra la información acerca de la amenaza: a qué tipo de activo afecta, qué dimensiones de los activos afecta y la descripción de la amenaza. El sistema genera una clave automática de riesgo, y solicita al usuario ingrese la información faltante. Se debe elegir a qué activos (de los registrados en el sistema) afecta el riesgo que se está registrando, para esto el sistema muestra una lista de la cual el usuario elige los activos. Cuando el usuario elige el número de incidentes ocurridos o la posibilidad de que el riesgo ocurra, el sistema es el encargado de otorgarle una calificación.

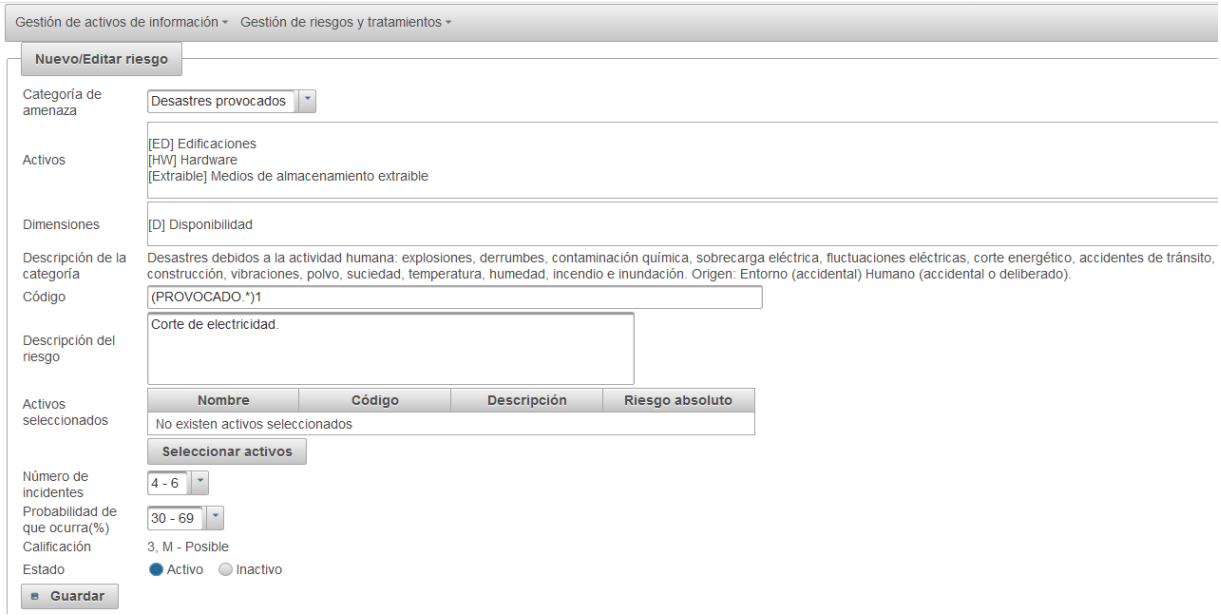

Ilustración 178: Registro o edición de riesgo.
Fuente: Elaboración propia.

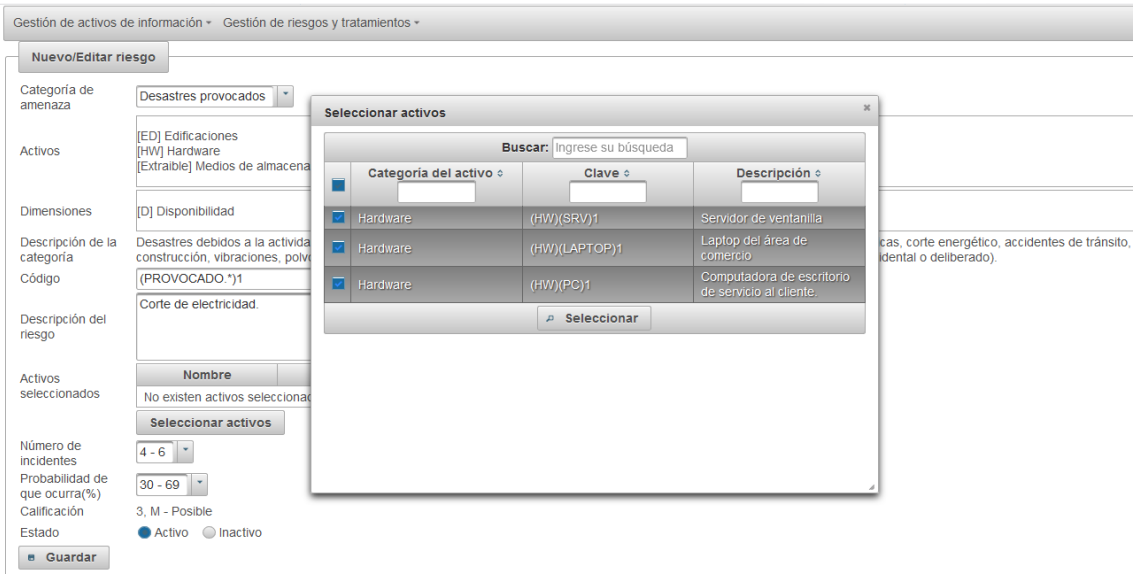

Ilustración 179: Registro o edición de riesgo, elección de activo.
Fuente: Elaboración propia.

El sistema lista todos los riesgos que hayan sido registrados y ofrece las opciones de "Editar" su información y consultar el "Detalle" de los registros.

Ilustración 180: Lista de riesgos registrados.
Fuente: Elaboración propia.

Continuando con la gestión de riesgos, el sistema relaciona cada activo cada riesgo con el cual haya sido relacionado. Se muestra una lista jerárquica, en la cual se calcula el riesgo acumulado y riesgo absoluto que representa ese riesgo en el activo; el cálculo del riesgo acumulado se basa en la multiplicación de la frecuencia del riesgo por el impacto en todas las dimensiones del activo; el riesgo absoluto es el mayor valor del riesgo acumulado, calculado anteriormente, sin embargo, el sistema únicamente realiza el cálculo del riesgo acumulado, en las dimensiones en que el activo se ve afectado por el riesgo.

Listado de activos por riesgo

Buscar por código de activo Buscar por código de riesgo

		VALOR							Impacto			Riesgo acumulado			Riesgo absoluto
Activo	Descripción	C	D	I	T	Riesgo	Descripción	Frecuencia	C	D	I	C	D	I	
(HW)(SRV)1	Servidor de vent	0	5	0	5										
			D			(N.*)1	Fuego	1	1	3	1	0	3	0	3
			D			(N.*)2	Inundaciones	3	1	3	1	0	3	0	9
			D			(PROVOCADO.*)1	Corte de electricidad.	3	1	3	1	0	3	0	9
(SW)(STD)(OS)2	Sistema operativ	5	7	7	7										
		C	D	I		(EL.1)1	Virus troyano	3	3	4	4	3	4	4	12
(HW)(LAPTOP)1	Laptop del área	9	7	6	9										
			D			(N.*)1	Fuego	1	5	4	4	0	4	0	4
			D			(PROVOCADO.*)1	Corte de electricidad.	3	5	4	4	0	4	0	12
(HW)(PC)1	Computadora de	5	3	4	5										
			D			(N.*)1	Fuego	1	3	3	3	0	3	0	3
			D			(N.*)2	Inundaciones	3	3	3	3	0	3	0	9
			D			(PROVOCADO.*)1	Corte de electricidad.	3	3	3	3	0	3	0	9

Ilustración 181: Lista de riesgos por activo.
Fuente: Elaboración propia.

La gestión de tratamientos, es manejado por el usuario coordinador de seguridad designado, para definir el plan de tratamiento se lo hace por medio de la lista jerárquica de riesgos por cada activo, presentada anteriormente, cuando un plan de tratamiento no ha sido definido, se habilita la opción de “Definir plan de tratamiento”, cuando el plan ya ha sido definido el sistema indica al usuario que ese riesgo “Si” tiene plan de tratamiento y habilita las opciones de consultar “Detalles del plan de tratamiento” o “Editar plan de tratamiento”.

Listado de activos por riesgo

Buscar por código de activo Buscar por código de riesgo

		VALOR							Impacto			Riesgo acumulado			Riesgo absoluto		
Activo	Descripción	C	D	I	T	Riesgo	Descripción	Frecuencia	C	D	I	C	D	I		Tratamiento	
(HW)(SRV)1	Servidor de vent	0	5	0	5												
			D			(N.*)1	Fuego	1	1	3	1	0	3	0	3	Si	
			D			(N.*)2	Inundaciones	3	1	3	1	0	3	0	9	Si	
			D			(PROVOCADO.*)1	Corte de electricidad.	3	1	3	1	0	3	0	9		
(SW)(STD)(OS)2	Sistema operativ	5	7	7	7												
		C	D	I		(EL.1)1	Virus troyano	3	3	4	4	3	4	4	12	Si	
(HW)(LAPTOP)1	Laptop del área	9	7	6	9												
			D			(N.*)1	Fuego	1	5	4	4	0	4	0	4	Si	
			D			(PROVOCADO.*)1	Corte de electricidad.	3	5	4	4	0	4	0	12		
(HW)(PC)1	Computadora de	5	3	4	5												
			D			(N.*)1	Fuego	1	3	3	3	0	3	0	3	Si	
			D			(N.*)2	Inundaciones	3	3	3	3	0	3	0	9	Si	
			D			(PROVOCADO.*)1	Corte de electricidad.	3	3	3	3	0	3	0	9		

Ilustración 182: Definir, editar o consultar plan de tratamiento.
Fuente: Elaboración propia.

En la definición o edición de un plan de tratamiento, el sistema requiere que se llenen y se escojan varios campos de información, entre ellos, la elección si es el plan es un tratamiento específico o un procedimiento normalizado, una vez elegido una opción el

sistema genera automáticamente la clave del plan de tratamiento; se define un cronograma de implementación del plan donde se definen actividades, responsables y semanas en qué se realiza dicha actividad; el plan de tratamiento requiere una fecha de próxima medición del riesgo, en la cual se evaluará y controlará el plan de tratamiento con respecto al riesgo.

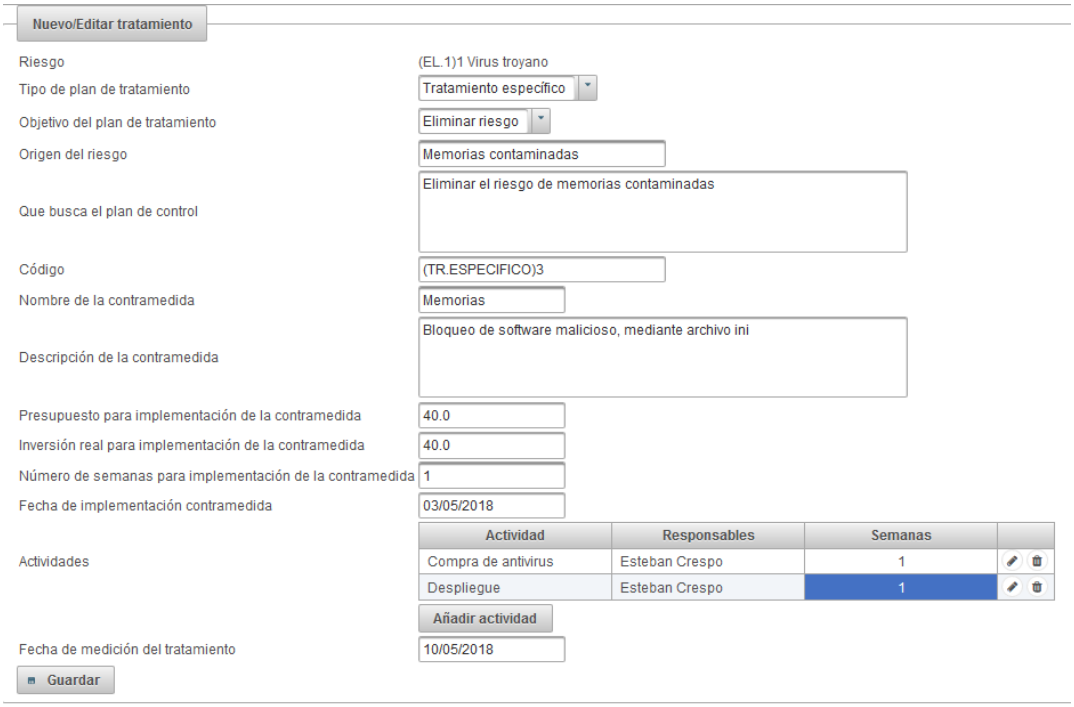

Ilustración 183: Definición o edición de plan de tratamiento.
Fuente: Elaboración propia.

En la lista de todos los planes de tratamiento existe la posibilidad de ver los "Detalles del plan de tratamiento", "Editar el plan de tratamiento" y la opción de "Medir el plan de tratamiento", la cual sólo está disponible cuando la fecha en que se intenta evaluar el plan sea igual o mayor a la fecha que se estableció anteriormente para medir el plan.

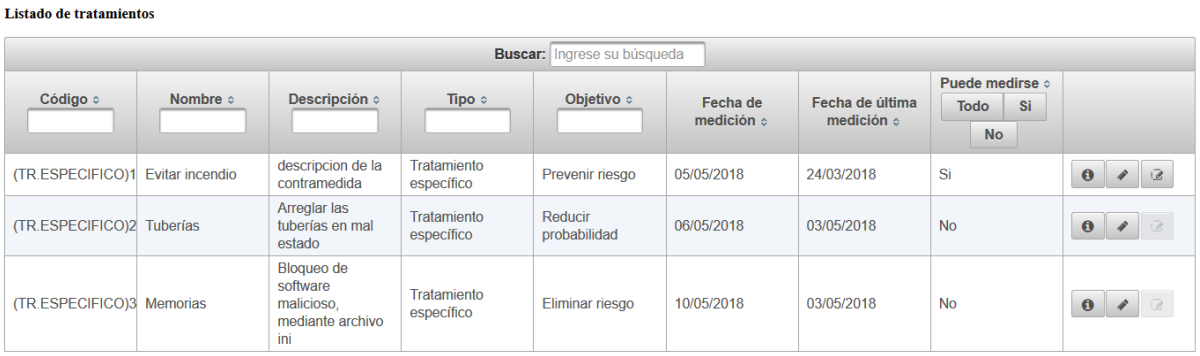

Ilustración 184: Listado de planes de tratamiento.
Fuente: Elaboración propia.

En le medición del plan de tratamiento, el sistema muestra la información del riesgo que es tratado y qué activos son afectados por ese riesgo, se ingresa el número de incidentes que han sido registrado o la probabilidad en porcentaje de que el riesgo se llegue a materializar, después que el plan de tratamiento haya sido implementado, el sistema automáticamente calificará al riesgo; se ingresa la fecha en que nuevamente se realizará una medición al plan de tratamiento.

Ilustración 185: Medición de plan de tratamiento.
Fuente: Elaboración propia.

El sistema emparenta cada activo de información con los riesgos relacionados a este y, estos riesgos presentan los planes de tratamiento que los mitigan; se presenta toda esta información mediante una lista jerárquica en donde se incluye el cálculo del riesgo acumulado, absoluto (indicado anteriormente) y el riesgo residual, el riesgo residual es la valorización del riesgo luego de que el plan de tratamiento haya sido implementado, se calcula su valor multiplicando la calificación de la frecuencia del riesgo otorgado en la evaluación del plan de tratamiento por cada una de las dimensiones del activo, se incluye las mismas restricciones que para el cálculo del riesgo acumulado, explicado anteriormente.

Listado de activos por riesgo - tratamiento

Buscar por código de activo | Buscar por código de riesgo | Buscar por código de tratamiento

		VALOR							Impacto			Riesgo acumulado			Riesgo absoluto			Impacto			Riesgo residual			Riesgo residual
Activo	Descripción	C	D	I	T	Riesgo	Descripción	Frecuencia	C	D	I	C	D	I		Contramedida	Descripción	Frecuencia	C	D	I	C	D	I	
(HW)(SRV)1	Servidor de ventanilla	0	5	0	5																				
			D			(N.*)1	Fuego	1	1	3	1	0	3	0	3	(TR.ESPECIFICO)1	Intalación de aspersores	1	1	3	1	0	3	0	3
			D			(N.*)2	Inundaciones	3	1	3	1	0	3	0	9	(TR.ESPECIFICO)2	Arreglar las tuberías en mal estado	1	1	3	1	0	3	0	3
			D			(PROVOCADO.*)1	Corte de electricidad.	3	1	3	1	0	3	0	9				1	3	1	0	3	0	
(SW)(STD)(OS)2	Sistema operativo Windows 8.1	5	7	7	7																				
		C	D	I		(EL.1)1	Virus troyano	3	3	4	4	3	4	4	12	(TR.ESPECIFICO)3	Bloqueo de software malicioso, median	1	3	4	4	3	4	4	4
(HW)(LAPTOP)1	Laptop del área de comercio	9	7	6	9																				
			D			(N.*)1	Fuego	1	5	4	4	0	4	0	4	(TR.ESPECIFICO)1	Intalación de aspersores	1	5	4	4	0	4	0	4
			D			(PROVOCADO.*)1	Corte de electricidad.	3	5	4	4	0	4	0	12				5	4	4	0	4	0	
(HW)(PC)1	Computadora de escritorio de servicio a	5	3	4	5																				
			D			(N.*)1	Fuego	1	3	3	3	0	3	0	3	(TR.ESPECIFICO)1	Intalación de aspersores	1	3	3	3	0	3	0	3
			D			(N.*)2	Inundaciones	3	3	3	3	0	3	0	9	(TR.ESPECIFICO)2	Arreglar las tuberías en mal estado	1	3	3	3	0	3	0	3
			D			(PROVOCADO.*)1	Corte de electricidad.	3	3	3	3	0	3	0	9				3	3	3	0	3	0	

Ilustración 186: Relación activos, riesgo y planes de tratamiento
Fuente: Elaboración propia.

Conclusiones del capítulo 8

El prototipo se centra en desarrollar el corazón del proceso de gestión de la metodología Ecu@Risk, es decir, se desarrolla la gestión de los activos de información, la gestión los riesgos de los activos y planes de tratamiento de los riesgos, además se presentan las relaciones entre activos, riesgos y planes de tratamiento, por medio de una lista la cual ha sido desarrollada para la fácil comprensión y análisis por parte de los usuarios; el prototipo tiene una interfaz muy amigable para el usuario, así como también, ha sido diseñado para que su usabilidad sea sencilla, cómoda e intuitiva y cumpla con toda la funcionalidad prevista en la etapa de diseño del sistema.

El prototipo no es el producto final, pero sirve para dar una idea clara de cómo funcionará el sistema de gestión de seguridad de la información, el objetivo es principal es simular el producto final, es decir, indicar cómo será el funcionamiento, cómo serán los cálculos de los riesgos, qué información presentará el sistema, así como, qué información se necesita registrar el sistema, etc. El prototipo da vida al diseño y a la idea de automatizar los procesos de gestión de la metodología para la gestión de riesgos Ecu@Risk, el prototipo siempre debe ir mejorando conforme se requiera hasta llegar al producto final que será entregado al cliente.

Conclusiones

En la actualidad, es obligación de las empresas buscar la manera de proteger y asegurar su información, debido a que, la información es una pieza clave y fundamental en las labores diarias de cualquier organización; y como lo señalan los autores Abril, Pulido y Bohada (2013), los ataques a los sistemas informáticos de las empresas son cada vez en mayor cantidad y más sofisticados. La gestión de riesgos de información ayuda a las empresas a identificar cuáles son sus vulnerabilidades, determinar qué riesgos podrían atacarlos, y también proporciona guías de cómo evaluar los riesgos identificados, y así las empresas definen qué riesgos pueden tratar, cuáles deben ser transferidos y cuáles pueden ser aceptados, para finalmente elaborar e implementar planes de mitigación hacia los riesgos, y de esta manera tener seguridad que la información de la empresa no se vea afectada y por consecuencia la empresa no será perjudicada.

La metodología Ecu@Risk desarrollada por Esteban Crespo (2016), presenta una gestión de riesgos muy entendible y adaptable a las empresas MPYMES, cubriendo todos los aspectos más importantes de la gestión de riesgos establecidas por normas y metodologías internacionales, lo que lo hace aplicable y viable en el entorno en el cual se desarrollan las empresas. La aplicación de la metodología promoverá el desarrollo de la conciencia y cultura de seguridad de información a en todas las empresas.

El sistema de gestión de seguridad de la información basado en la metodología Ecu@Risk fue pensado para funcionar en la red, debido a esto, para el establecimiento de sus directrices de elaboración se tomó como base teórica la guía de ingeniería de software orientada a la red llamada “ingeniería web”, esta guía fue propuesta por la autora García Chi (2013), en la cual como áreas principales se encuentran: la formulación del sistema (metas y objetivos), la recopilación de requisitos del sistema, y el modelado en sí del sistema. Para la formulación y recopilación de requisitos del sistema se estudiaron y aplicaron los conceptos dados en la guía de especificación de requisitos del estándar IEE 830 (2008) y para el modelado del sistema (modelo de contenido, interacción, funcional, configuración y navegación), se aplicaron los conceptos de la programación orientado a objetos, los cuales fueron adquiridos durante los años de estudio de la carrera. Es decir, los fundamentos teóricos para la elaboración de las directrices del sistema, están basados principios de ingeniería y buenas prácticas.

El levantamiento de requisitos de un sistema es el inicio del ciclo de vida del software y es la parte más importante de éste, ya que en él se define el alcance que tendrá el software, cuáles serán los objetivos, su funcionalidad, etc. Para la definición de los requisitos del sistema Ecu@Risk se estableció un orden de actividades: primero se analizó a profundidad el funcionamiento de la metodología de gestión de riesgos Ecu@Risk, se estudiaron los procesos y procedimientos de: identificación y valoración de los activos de información , el reconocimiento de amenazas, la definición y valoración de los riesgos, el cálculo y valoración de los riesgos residuales y absolutos, el establecimiento de planes de tratamiento para los riesgos, el cálculo y valoración del riesgo residual, y finalmente, la definición de procesos de negocio; el siguiente paso fue decidir qué y cómo se pueden automatizar los procesos de la metodología. La segunda actividad realizada fue la elaboración de una guía de evaluación de software, aplicando el estándar internacional ISO/IEC 9126, el propósito de esta guía es evaluar y comparar programas informáticos que estén vigentes en el mercado, los cuales puedan gestionar riesgos de información; cabe recalcar que esta guía fue elaborada en base al funcionamiento de la metodología Ecu@Risk; con este análisis se obtuvo una idea clara de cómo funcionan los programas de gestión de riesgos de información, y en base a esto fueron levantados los requerimientos que finalmente tendrá el sistema de gestión de riesgos a desarrollarse. La última actividad fueron las reuniones con el creador de la metodología Esteban Crespo, en estas reuniones se realizan cambios y aprobaciones a los requerimientos levantados del sistema. Con el desarrollo de todas estas actividades se establecieron las directrices claras de cómo realizar el levantamiento y modelamiento del sistema Ecu@Risk.

La codificación e implementación del sistema de gestión de seguridad de la información que fue diseñado es un proyecto, el cual requiere directrices de cómo ser gestionado; la gestión de proyectos proporciona guías de cómo llevar a cabo el proyecto. Se debe definir una metodología de gestión de proyectos; el sistema Ecu@Risk opta por una metodología ágil (Scrum), ya que proporciona todas las características que el sistema requiere para su desarrollo: rápida respuesta al cambio, el tiempo de elaboración, una planificación que puede adaptarse al equipo de desarrollo, etc. Después de la elección de una metodología de desarrollo se define un cronograma de actividades y se establece el tiempo que se necesita para la elaboración de un proyecto. El presupuesto para el desarrollo de un proyecto, es una parte muy importante en la planificación de un proyecto, puesto que se trata, de la manera en cómo se solventarán los costos de los recursos, que son necesarios para la realización del proyecto; el sistema

Ecu@Risk es dirigido para empresas del sector MPYMES, por lo tanto, se ha buscado elaborar el sistema licencias de software libre, y cotizando únicamente las actividades a realizarse para la construcción del sistema. Finalmente los riesgos siempre estarán presentes en la elaboración de un proyecto, poder gestionarlos y solventarlos sin perjudicar el desarrollo normal del proyecto puede definir un proyecto exitoso o un fracaso; la gestión de riesgos del proyecto es la planificación de respuesta ante cualquier adversidad que se pueda presentar durante el desarrollo del proyecto; se establece una lista de posibles riesgos que se puedan suscitar, sin embargo, esta lista no es definitiva, puede ir ampliándose de acuerdo a cada proyecto así también su plan de respuesta deberá ser actualizado. Las directrices de gestión del proyecto de desarrollo del sistema se centran en la planificación del proyecto, presupuesto y gestionar los riesgos.

Finalmente, el prototipo del software da vida a las directrices propuestas en este trabajo para la elaboración de un sistema de gestión de seguridad de la información, y a la idea de automatizar los procesos de gestión de la metodología para la gestión de riesgos Ecu@Risk, el prototipo siempre debe ir mejorando conforme se requiera hasta llegar al producto final que será entregado al cliente.

Trabajos futuros

El prototipo de software de soporte basado en la metodología podría ser desarrollado y perfeccionado hasta lograr una versión distribuible. Adicional a este trabajo, uno de los aspectos que deberían ser considerados en un trabajo futuro es el de realizar una propuesta para la valoración monetaria de los activos de información, basada en el método Montecarlo. Esta valoración permitiría conocer el impacto de la materialización de una amenaza no solamente en aspectos de disponibilidad, confidencialidad e integridad; sino que además permitiría identificar el impacto económico en la organización. Así, la aplicación podría no solo apoyar a la gestión de riesgo de información, sino que además potenciaría el impulsar programas de mitigación de amenazas, pues muchas veces el impacto económico es lo que más interesa a los gerentes o propietarios de una empresa.

Bibliografía

Abril, A., Pulido, J., & Bohada, J. (2013). Análisis de riesgos en seguridad de la información. *Revista Ciencia, Innovación y Tecnología (RCIYT)*, 39-53.

Amaya Balaguera, Y. D. (2013). Metodologías ágiles en el desarrollo de aplicaciones para dispositivos móviles. Estado actual. *Revista de Tecnología, ISSN 1692-1399, Vol. 12, Nº. 2*, 111-123.

Cabot Segarra, J. (2013). *Ingeniería del software.* Barcelona, España: Editorial UOC.

Cochea Tomalá, S. J. (2009). *Métricas de Calidad de los Sistemas de Información – aplicación en la Certificación de Calidad de un Sistema de una empresa del sector hidrocarburífero.* Tesis de pregrado, Escuela Superior Politécnica del Litoral, Guayaquil.

Crespo, E. (2016). *ECU@Risk Una metodología para la gestión de riesgo aplicada a las MPYMES del Ecuador.* Tesis de postgrado, Universidad de Cuenca, Facultad de Ingeniería, Cuenca.

EAR/PILAR. (s.f.). *EAR / PILAR análisis de riesgos*. Recuperado el 10 de 26 de 2017, de http://www.ar-tools.com/es/tools/pilar/v62/index.html

Fernández Sanz, L., & Bernad Silva, P. (2014). Gestión de riesgos en proyectos de desarrollo de software en España: estudio de la situación. *Revista Facultad de Ingeniería Universidad de Antioquia N. º70* , 233-243.

Ferré Grau, X., & Sánchez Segura, M. I. (2014). *Desarrollo Orientado a Objetos con UML*. Guía técnica, Universidad Politécnica de Madrid, Facultad de informática, Madrid.

García Chi, R. I. (2013). *Guía técnica de ingeniería Web.* Guía Técnica, Instituto Tecnológico de Ciudad Valles, Departamento de sistemas y computación, Ciudad Valles.

Gómez Rueda, J. (2016). *Dirección y gestión de proyectos de Tecnologías de la Información en la empresa.* Madrid: FC Editorial.

IEEE. (2008). *Especificación de Requisitos según el estándar IEEE 830.*

INCIBE. (s.f.). *INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA*. Recuperado el 28 de 10 de 2017, de https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

Kendal, K. (2011). *Análisis y Diseño de Sistemas 8va. Edición.* Mexico: Prentice Hall.

Largo García, C. A., & Marin Mazo, E. (2005). *Guía técnica para evaluación de software.* Guía técnica.

Montoya, M., Pulgarín, E., & Monsalve, J. C. (2014). Estratégias didácticas en el aprendizaje para el levantamiento de requerimientos. En A. S. Arango, *La investigación, un compromiso con la sociedad* (págs. 393-400). Medellín: Fondo Editorial Luis Amigó.

Muhairat, M., Alrawashdeh, T. A., & Althunibat , A. (2013). Evaluating the Quality of Software in ERP. *International Journal of Ambient Systems and Applications (IJASA) Vol.1, No.1*.

MySQL. (s.f.). *MySQL Workbench*. Recuperado el 01 de 03 de 2018, de https://www.mysql.com/products/workbench/

Navarro Cadavid, A., Fernández Martínez, J. D., & Morales Vélez, J. (2013). Revisión de metodologías ágiles para el desarrollo de software. *Prospect. Vol. 11, No. 2*, 30-39.

PM4DEV. (2009). Gestión del presupuesto del proyecto. *Una metodología para la gerencia de proyectos de desarrollo en organizaciones de asistencia internacional y apoyo humanitario*.

Project Management Institute. (2004). *"A guide to the Project Management Body of Knowledge: (PMBOK guide)".* Project Management Institute.

Ramírez Zuluaga, C. M. (2011). *INTEGRACIÓN ENTRE PSP Y PMBOK® APLICADA AL DESARROLLO DE UN SISTEMA EXPERTO PARA EL DIAGNÓSTICO E IDENTIFICACIÓN AUTOMÁTICA DE ENFERMEDADES PROFESIONALES.* Tesis de postgrado, Universidad Autónoma de Manizales, Manizales.

Rodríguez, S. S. (2012). *Metodología para la gestión del riesgo en proyectos.* Tesis de pregado, Escuela Politécnica Superior, Universiad Autónoma de Madrid, Departamento de Tecnología Electrónica y de las Comunicaciones, Madrid.

Rumbaugh, J., Jacobson, I., & Booch, G. (2004). *The Unified Modeling Language Reference Manual Second Edition.* Boston : Pearson Education,Inc.

Schwaber, K., & Sutherland, J. (2013). *La Guía Definitiva de Scrum: Las Reglas del Juego.* Guía técnica.

SimpleRisk. (07 de 04 de 2017). *SimpleRisk.* Recuperado el 27 de 10 de 2017, de https://www.simplerisk.com/blog/the-origin-of-simplerisk-a-founders-story

Sullivan, P. (2016). *TechTarget.* Recuperado el 31 de 05 de 2017, de SearchDataCenter en Español: http://searchdatacenter.techtarget.com/es/consejo/Gestion-de-riesgos-de-seguridad-de-la-informacion-Comprension-de-los-componentes

Trigas Gallego, M. (s.f.). Metodología SCRUM. Recuperado el 2018 de 03 de 15, de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/17885/1/mtrigasTFC0612memoria.pdf

Vidal, C., Schmal, R., Rivero, S., & Villaroel, R. (2012). Extensión del Diagrama de Secuencias UML (Lenguaje de Modelado Unificado) para el Modelado Orientado a Aspectos. *Información Tecnológica*, 51-62.

Anexos

Decano de la Facultad de Ciencias de la Administración, Cuenca, 24 de noviembre de 2017.- Con autorización amplia y suficiente concedida por el Consejo de Facultad en sesión del 25 de febrero de 2016, conoció la petición de la estudiante **PABLO ANDRES CEVALLOS ORDOÑEZ** con código 65662, quien solicita prórroga para la presentación del trabajo de titulación denominado: "***DIRECTRICES PARA LA CONSTRUCCIÓN DE UN SOFTWARE Y ADMINISTRACIÓN DE UN PROYECTO PARA UN SGSI, BASADO EN LA METODOLOGIA ECU@RISK***", previo a la obtención del título de Ingeniero de Sistemas y Telemática, cuyo plazo de presentación vence el 29 de noviembre de 2017, en apego al Reglamento de Régimen Académico y la normativa Institucional, *resuelve aprobar la solicitud y conceder una prórroga de seis meses, esto es* ***hasta el 29 de mayo de 2018.***

Ing. Oswaldo Merchán Manzano
Decano de la Facultad de
Ciencias de la Administración

rcr.-

.Doctora Jenny Ríos Coello, Secretaria de la Facultad de Ciencias de la Administración de la Universidad del Azuay

C E R T I F I C A:

Que, el Consejo de Facultad en sesión del 29 de mayo de 2017, conoció la petición del estudiante **PABLO ANDRÉS CEVALLOS ORDÓÑEZ** con código **65662**, que presenta el diseño de su trabajo de titulación denominado: "***DIRECTRICES PARA LA CONSTRUCCIÓN DE UN SOFTWARE Y ADMINISTRACIÓN DE UN PROYECTO PARA UN SGSI, BASADO EN LA METODOLOGÍA ECU@RISK***", presentado previa a la obtención del título de Ingeniero de Sistemas y Telemática.- El Consejo de Facultad acogió el informe de la Junta Académica de Ingeniería de Sistemas y Telemática y resolvió aprobar el diseño. Designa como **Director al ingeniero Esteban Crespo Martínez** y como miembros del Tribunal Examinador al ingeniero Francisco Salgado Arteaga, Ph.D. e ingeniera Catalina Astudillo Rodríguez.- En esta misma sesión el Consejo de Facultad fija como plazo para la entrega del trabajo de titulación, seis meses contados desde la fecha de su aprobación, esto es hasta el **29 de noviembre de 2017,** debiendo el Director presentar a la Junta Académica, dos informes bimensuales del desarrollo del trabajo de titulación.

Cuenca, mayo 30 de 2017

Dra. Jenny Ríos Coello
Secretaria de la Facultad de
Ciencias de la Administración

CONVOCATORIA

Por disposición de la Junta Académica de **Ingeniería de Sistemas y Telemática**, se convoca a los Miembros del Tribunal Examinador, a la sustentación del Protocolo del Trabajo de Titulación: **"DIRECTRICES PARA LA CONSTRUCCIÓN DE UN SOFTWARE PARA LA GESTIÓN DEL RIESGO DE INFORMACIÓN, BASADO EN LA METODOLOGÍA ECU@RISK"**, presentado por el estudiante **Pablo Andrés Cevallos Ordóñez**, previa a la obtención del grado de **Ingeniero en Sistemas y Telemática**, para el día **MARTES 16 DE MAYO DE 2017 A LAS 11h00,** La sustentación se realizará en el **laboratorio del IERSE.**

Cuenca, 11 de mayo de 2017

Dra. Jenny Ríos Coello
Secretaria de la Facultad

Ing. Esteban Crespo Martínez .....

Ing. Catalina Astudillo Rodríguez .....

Dr. Francisco Salgado Arteaga .....

mjmr/

Comunicado OK.

Facultad de Ciencias de la Administración
Escuela de Ingeniería de Sistemas y Telemática

Oficio Nro. 065-2017-DIST-UDA

Cuenca, 12 de mayo de 2017

Señor Ingeniero
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 12 de mayo del 2017, recibió el proyecto de tesis titulado "Directrices para la construcción de un software para la gestión del riesgo de información, basado en la metodología ECU@Risk", presentado por Pablo Andrés Cevallos Ordóñez estudiante de la Escuela de Ingeniería de Sistemas y Telemática, y revisado por el Ing. Esteban Crespo, previo a la obtención del título de Ingeniero de Sistemas y Telemática.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomendamos como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior al Ing. Esteban Crespo y como miembros del Tribunal a Francisco Salgado Ph.D. e Ing. Catalina Astudillo.

Atentamente,

Ing. Marcos Orellana Cordero
Cordinador Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay

UNIVERSIDAD DEL AZUAY

ACTA
SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

1.1 **Nombre del estudiante:** **Pablo Andrés Cevallos Ordóñez**
1.2 **Director sugerido**: Ing. Esteban Crespo Martínez
1.3 **Codirector (opcional)**:
1.4 **Tribunal:** Ing. Catalina Astudillo Rodríguez/ Dr. Francisco Salgado Arteaga
1.5 **Título propuesto: "DIRECTRICES PARA LA CONSTRUCCIÓN DE UN SOFTWARE PARA LA GESTIÓN DEL RIESGO DE INFORMACIÓN, BASADO EN LA METODOLOGÍA ECU@RISK"**
1.6 **Resolución**:

1.6.1 Aceptado sin modificaciones X

1.6.2 Aceptado con las siguientes modificaciones:

CAMBIAR EL TÍTULO A "DIRECTRICES PARA LA CONSTRUCCIÓN DE UN SOFTWARE Y ADMINISTRACIÓN DE UN PROYECTO PARA UN SGSI, BASADO EN LA METODOLOGÍA ECU@RISK"

1.6.3 Responsable de dar seguimiento a las modificaciones: Ing. Esteban Crespo

1.6.4 No aceptado
- Justificación:

Tribunal

Ing. Esteban Crespo Martínez — Ing. Catalina Astudillo Rodríguez — Dr. Francisco Salgado Arteaga

Pablo Cevallos
Sr. Pablo Andrés Cevallos Ordóñez

Dra. Jenny Ríos Coello
Secretario de Facultad

Fecha de sustentación: día **MARTES 16 DE MAYO DE 2017 A LAS 11h00**

UNIVERSIDAD DEL AZUAY

RÚBRICA PARA LA EVALUACIÓN DEL PROTOCOLO DE TRABAJO DE TITULACIÓN

1.1 Nombre del estudiante: Pablo Andrés Cevallos Ordóñez
1.2 Director sugerido: Ing. Esteban Crespo Martínez
1.3 Codirector (opcional):
1.4 Título propuesto: **"DIRECTRICES PARA LA CONSTRUCCIÓN DE UN SOFTWARE PARA LA GESTIÓN DEL RIESGO DE INFORMACIÓN, BASADO EN LA METODOLOGÍA ECU@RISK"**
1.5 Revisores (tribunal): Ing. Catalina Astudillo Rodríguez/ Dr. Francisco Salgado Arteaga
1.6 Recomendaciones generales de la revisión:

	Cumple totalmente	Cumple parcialmente	No cumple	Observaciones (*)
Línea de investigación				
1. ¿El contenido se enmarca en la línea de investigación seleccionada?	✓			
Título Propuesto				
2. ¿Es informativo?				
3. ¿Es conciso?	✓			
Estado del arte				
4. ¿Identifica claramente el contexto histórico, científico, global y regional del tema del trabajo?	✓			
5. ¿Describe la teoría en la que se enmarca el trabajo	✓			
6. ¿Describe los trabajos relacionados más relevantes?	✓			
7. ¿Utiliza citas bibliográficas?	✓			
Problemática y/o pregunta de investigación				
8. ¿Presenta una descripción precisa y clara?	✓			
9. ¿Tiene relevancia profesional y social?	✓			
Hipótesis (opcional)				
10.¿Se expresa de forma clara?				N/A
11.¿Es factible de verificación?				N/A
Objetivo general				
12.¿Concuerda con el problema formulado?	✓			
13.¿Se encuentra redactado en tiempo verbal infinitivo?	✓			

Objetivos específicos				
14.¿Concuerdan con el objetivo general?	/			
15.¿Son comprobables cualitativa o cuantitativamente?	/			
Metodología				
16.¿Se encuentran disponibles los datos y materiales mencionados?	/			
17.¿Las actividades se presentan siguiendo una secuencia lógica?	/			
18.¿Las actividades permitirán la consecución de los objetivos específicos planteados?	/			
19.¿Los datos, materiales y actividades mencionadas son adecuados para resolver el problema formulado?	/			
Resultados esperados				
20.¿Son relevantes para resolver o contribuir con el problema formulado?	/			
21.¿Concuerdan con los objetivos específicos?	/			
22.¿Se detalla la forma de presentación de los resultados?	/			
23.¿Los resultados esperados son consecuencia, en todos los casos, de las actividades mencionadas?	/			
Supuestos y riesgos				
24.¿Se mencionan los supuestos y riesgos más relevantes?	/			
25.¿Es conveniente llevar a cabo el trabajo dado los supuestos y riesgos mencionados?	/			
Presupuesto				
26.¿El presupuesto es razonable?				N/A
27.¿Se consideran los rubros más relevantes?				N/A
Cronograma				
28.¿Los plazos para las actividades son realistas?	/			
Referencias				
29.¿Se siguen las recomendaciones de normas internacionales para citar?	/			
Expresión escrita				
30.¿La redacción es clara y fácilmente comprensible?	/			
31.¿El texto se encuentra libre de faltas ortográficas?	/			

(*) Breve justificación, explicación o recomendación.

- Opcional cuando cumple totalmente,
- Obligatorio cuando cumple parcialmente y NO cumple.

.....

.....

.....

.....	.....	.....
Ing. Esteban Crespo Martínez	Ing. Catalina Astudillo Rodríguez	Dr. Francisco Salgado Arteaga

Cuenca, 17 de mayo de 2017

Ingeniero,
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
UNIVERSIDAD DEL AZUAY

De mi consideración,

Yo **Paúl Esteban Crespo Martínez** informo que he revisado los cambios realizados al protocolo del trabajo de titulación previo a la obtención del título de Ingeniero/Ingeniera en Sistemas y Telemática, denominado **"Directrices para la construcción de un software y administración de un proyecto para SGSI basado en la metodología ECU@Risk "**, elaborado por la/el estudiante **Pablo Andrés Cevallos Ordoñez**, con código/s estudiantil 65662. Trabajo que según mi criterio cumple con las modificaciones sugeridas por el Tribunal y puede continuar su desarrollo planificado.

Sin otro particular, suscribo

Atentamente

Paúl Esteban Crespo Martínez

UNIVERSIDAD DEL AZUAY

DOCTORA JENNY RIOS COELLO, SECRETARIA DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION DE LA UNIVERSIDAD DEL AZUAY

C E R T I F I C A:

Que, el señor **CEVALLOS ORDOÑEZ PABLO ANDRES,** con código **65662,** alumno de la escuela de **INGENIERIA DE SISTEMAS Y TELEMATICA**, tiene aprobado más del 80% de los créditos de su malla de estudios.

Que, al señor **CEVALLOS ORDOÑEZ PABLO ANDRES,** le falta aprobar las siguientes asignaturas para finalizar sus estudios:

PRODUCCIÓN II

SISTEMAS DE INFORMACIÓN GERENCIAL

PROYECTOS TELEMÁTICOS

CALIDAD DE SOFTWARE

INGENIERÍA DE SOFTWARE II

METODOLOGIA DE LA INVESTIGACION

Cuenca, 10 de mayo de 2017

Derecho No. **001-001-000156879**

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 Nº 0792622

Cuenca, 10 de mayo de 2017

Ingeniero

Oswaldo Merchán

Decano de la Facultad de Ciencias de la Administración

Presente

De mi consideración:

Por la presente, me permito informarle que he revisado el diseño de tesis presentado por el estudiante **Pablo Andrés Cevallos Ordóñez** con código **65662** y con el tema *"Directrices para la construcción de un software para la gestión del riesgo de información, basado en la metodología ECU@Risk"*, como requisito previo para la obtención del título de Ingeniero de Sistemas y Telemática.

Al respecto, el diseño de tesis presenta una estructura teórica, metodológica y técnica coherente, cuyo objetivo es el de proponer directrices para la construcción de un software que permita gestionar los riesgos de información, considerando la teoría de la ingeniería de software y la metodología ECU@Risk, alineándose al proyecto del libro "Metodología para la gestión de riesgos de información" que ejecuto actualmente en la Universidad del Azuay.

Por lo expuesto, emito informe favorable y recomiendo su aprobación.

Esteban Crespo Martínez

Docente de la Universidad del Azuay

UNIVERSIDAD DEL AZUAY

Escuela Sistemas y Telemática	Oficio Estudiante: Solicitud aprobación de Protocolo de Trabajo de Titulación	IST-RE-EST-02 Versión 01 04/04/2017 Página 1 de 1

Lugar de Almacenamiento	Retención	Disposición Final
F: Archivo Secretaría de la Facultad	5 años	Almacenar en archivo pasivo de la Facultad

Cuenca, 12 de mayo de 2017

Ingeniero,
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
UNIVERSIDAD DEL AZUAY

De mi consideración,

Estimado Señor Decano, yo **Pablo Andrés Cevallos Ordóñez** con C.I. **0105600480**, código estudiantil **65662** estudiante de la Carrera de Sistemas y Telemática, solicito muy comedidamente a usted y por su intermedio al Consejo de Facultad, la aprobación del protocolo de trabajo de titulación con el tema **"DIRECTRICES PARA LA CONSTRUCCIÓN DE UN SOFTWARE PARA LA GESTIÓN DEL RIESGO DE INFORMACIÓN, BASADO EN LA METODOLOGÍA ECU@RISK"** previo a la obtención del título de Ingeniero en Sistemas y Telemática para lo cual adjunto la documentación respectiva.

Por la favorable acogida que brinde a la presente, anticipo mi agradecimiento

Atentamente:

Pablo Cevallos

Pablo Andrés Cevallos Ordóñez

Estudiante de la Carrera de Sistemas y Telemática

Edición autorizada de 10.000 ejemplares
Del 778.501 al 788.500 Nº 0785911

UNIVERSIDAD DEL AZUAY

UNIVERSIDAD DEL AZUAY
INGENIERIA EN SISTEMAS Y TELEMATICA
DISEÑO DE TESIS

1. DATOS GENERALES

1.1 Nombre del estudiante: Cevallos Ordóñez Pablo Andrés

1.1.1 Código:65662

1.1.2 Contacto:

Teléfono convencional: 2880842

Celular: 0984241370

Correo electrónico: ua065662@uazuay.edu.ec

1.3 Director sugerido: Crespo Martínez, Esteban Ing.

1.2.1 Contacto:

Teléfono convencional: 4092109

Celular:0996804562

Correo electrónico: ecrespo@uazuay.edu.ec

1.3 Co-director sugerido:

1.4 Asesor metodológico: Salgado Arteaga Francisco, PhD.

1.5 Tribunal designado:

1.6 Aprobación: Junta Académica:

Consejo de Facultad:

1.7 Línea de Investigación de la carrera:

1.7.1 Código UNESCO:1203 Informática de computadores

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 Nº 0796603

1.7.2 Tipo de trabajo: Investigación aplicada.

1.8 Área de estudio: Ingeniería de software, Seguridad de la información.

1.9 Título propuesto: Directrices para la construcción de un software y administración de un proyecto para un SGSI, basado en la metodología ECU@Risk.

1.10 Subtítulo:

1.11 Estado del proyecto: Continuación de la investigación relacionada con el desarrollo de una metodología para la gestión de riesgos de información aplicada a las MPYMES.

2. CONTENIDO

2.1 Motivación de la investigación:

Proponer líneas de desarrollo de un software que permita la gestión de riesgos de información basado en la metodología Ecu@Risk; metodología relativamente nueva utilizada en la gestión de riesgos de información, cuyo objetivo es identificar los activos de información y las amenazas que podrían colocar a las MPYMES ecuatorianas en escenarios de riesgo de información. Bajo este preámbulo, se puede decir que dicha metodología aún no tiene desarrollado un software que soporte a todos sus procesos de gestión.

2.2 Problemática:

Muchas aplicaciones informáticas para la gestión de riesgos que se ofertan en el mercado tienen un precio elevado y, por lo tanto, lejos del alcance de una MPYME. Esto hace que las empresas no la consideren como una necesidad o política prioritaria en cuanto a la protección de su información.

La metodología Ecu@Risk es precisamente desarrollada para la aplicación de gestión de riesgos de información para las MPYMES, sin embargo, aún no cuenta con los lineamientos para la construcción de un software que facilite su aplicación.

2.3 Pregunta de investigación:

¿Cómo la ingeniería de software puede apoyar a la seguridad de la información en el desarrollo de una aplicación que permita gestionar los riesgos de la información?

2.4 Resumen:

El proyecto consiste en proponer los lineamientos para la construcción de un software para la gestión de riesgos de información mediante la aplicación de ingeniería de software, partiendo del levantamiento de requerimientos, siguiendo con diseño del software, la gestión del proyecto de desarrollo y culminando con la gestión de calidad del proyecto.

2.5 Indagación exploratoria:

Según (Abril, Pulido, & Bohada, 2013) las Tecnologías de información, servicios y modelos de comunicación e información, y el incremental uso globalizado de Internet, ha llevado a que se aumenten los ataques a los sistemas informáticos de las empresas y organizaciones, tratando de comprometer su información, la misma que es considerada como un recurso vital, y que debe responder siempre a los principios de la seguridad de la información que son: integridad, disponibilidad y confidencialidad (Crespo, 2016);

Los crecientes ataques a los sistemas de información han llevado a las empresas a buscar estrategias que permitan analizar herramientas y contramedidas que ayuden prevenir, controlar,

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 Nº 0797218

reducir, mitigar, transferir o aceptar riesgos que se asocian a la violación o vulneración de la información.(Abril, Pulido, & Bohada, 2013)

Coincidiendo con las palabras de Dmitry Bestuzhev especialista en seguridad informática quien dijo que "A pesar de que se han hecho esfuerzos, (en Ecuador) todavía no se trabaja en seguridad de manera sistemática con políticas definidas. El Gobierno no tiene un plan de acciones para todas las entidades del país. Muchas veces es el propietario o el administrador del sitio web el que decide qué hacer para que este sea seguro, por ello Ecuador llega a ser un blanco fácil de los atacantes" (Delgado, 2014), se puede decir que en Ecuador la seguridad de la información es algo casual donde no se ha desarrollado una cultura de seguridad.

En un estudio realizado por (Crespo, 2016), se puede ver que en el entorno ecuatoriano la micro, pequeña y mediana empresa (MPYME) no tiene una estrategia o metodología para la gestión de Riesgos de Información que considere la realidad nacional ecuatoriana. Algunas Instituciones de control tratan de implementar prácticas internacionales, pero fracasan debido a la cantidad de exigencias de parámetros y procedimientos que las norman requieren.

(Crespo, 2016) desarrolla una metodología para la gestión de Riesgos de Información que se adapta al entorno ecuatoriano y que puede ser aplicada a las MPYMES, llamada Ecu@Risk, esta metodología proporciona directrices para:

- Identificar el contexto organizacional.
- Registrar los activos de información.
- Identificar y valorar los riesgos y amenazas físicas, de entorno, y lógicas.
- Directrices para el desarrollo de contramedidas y políticas de seguridad.

Ecu@Risk tiene como fundamentos teóricos otras metodologías como: Magerit V3, Microsoft Risk Management, Octave-S y CRAMM, Ecu@Risk está alineada a marcos de gestión como COBIT 5 y COSO III y a las normas internacionales ISO 27001, ISO 27002, ISO 27003 e ISO 27005 (Crespo, 2016).

La metodología señalada anteriormente requiere de un software para que sus procesos, procedimientos y actividades sean registradas, evaluadas y controladas correctamente. Para el desarrollo de este, se requiere el empleo de las técnicas que sugiere la Ingeniería de software, empezando por la identificación o levantamiento de requisitos, elementos que ayudan a entender el problema, delimitar el alcance de la propuesta, entre otros aspectos.(Montoya, Pulgarín, & Monsalve, 2014). Existen muchos métodos y técnicas para levantar requerimientos, sin embargo, se debe analizar y escoger el que mejor se adapte a la situación, considerando que el desarrollo de software necesita de un amplio análisis, en donde los requerimientos del cliente deben estar correctamente estructurados e identificados. (Montoya, Pulgarín, & Monsalve, 2014)

Siguiendo con el desarrollo de la ingeniería de software se debe realizar el diseño de la aplicación. El lenguaje de modelo unificado (UML) ayuda a traducir los requisitos levantados en

representaciones de desarrollo de software orientado a objetos (DSOO), modularizando los principales elementos estructurales y de comportamiento y las relaciones entre ellos de una aplicación software. El UML permite la modelación tanto de componentes estáticos, así como de componentes dinámicos del software (Vidal, Schmal, Rivero, & Villaroel, 2012). En esta etapa se maneja también el diseño de datos, interfaz hombre-usuario, entre otras.

Para que la construcción del software sea satisfactoria y cumpla con todas las expectativas trazadas en él, es preciso gestionar el proyecto de construcción de dicho software. Así responderemos algunas preguntas claves que surgen tales como: ¿Cuál será el plazo de entrega?, ¿Cuánto costará?, ¿Qué recurso humano requiere?, etc. (Carranza, 2016). Para llevar a cabo la gestión del proyecto, se debe contar con una correcta planificación del mismo con puntos casos de uso, WBS (WorkBreakdownStructure), etc.; así mismo, tener un correcto análisis financiero, dirá si el proyecto es viable o no. Por otro lado, también es importante contar con la programación temporal de proyecto (diagramas de Gantt y Pert).

Adicionalmente, se debe realizar un análisis de riesgos, para garantizar que el proyecto está preparado para solventar cualquier contratiempo que se pueda presentar. La gestión de riesgo de proyectos según (Pérez & Zulueta, 2013), consta de: i) la planificación de la gestión de riesgos, ii) identificar riesgos y amenazas, iii) analizar los riesgos, iv) definir y aplicar actividades para la resolución de eventualidades, v) comunicar los riesgos y vi) evaluar el proceso de gestión de riesgos.

La obtención de un producto software de calidad implica que sean utilizadas metodologías o procedimientos estandarizados para el análisis, diseño, programación y prueba del software, haciendo que el software cumpla estándares de calidad tanto en el desarrollo como en el control mismo de calidad (Osorio & Castro, 2011).

La planeación del software debe ser comprendida, estudiada, usada y ser atractiva para el usuario, cumpliendo con la definición de usabilidad de software que exponen (Mascheroni, Greiner , Petris, Dapozo, & Estayno, 2012). Apoyados en los atributos de usabilidad, el software debe tener:

- Facilidad de aprendizaje.
- Eficiente.
- Manejo de errores
- Presentación visual apropiada
- Satisfacción.

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 Nº 0797217

2.6 Objetivo general:

Proponer directrices para la construcción de un software que permita gestionar los riesgos de información considerando la teoría de la ingeniería de software y la metodología ECU@Risk.

2.7 Objetivos específicos:

1. Fundamentar teóricamente los componentes que permiten el análisis y desarrollo de software bajo principios de ingeniería y buenas prácticas de aseguramiento y calidad.
2. Proponer directrices para levantamiento de requisitos, y el modelamiento del software.
3. Proponer directrices para la gestión del proyecto, contemplando los riesgos que pueden presentarse durante el desarrollo del software para gestión de riesgos de información.

2.8 Metodología:

Se aplicarán los conocimientos adquiridos durante los años de estudio de la carrera relacionados con Ingeniería de software y seguridad de la información, específicamente los relacionados con la gestión de riesgos de la información.

Se estudiará e identificará los fundamentos teóricos de la metodología Ecu@Risk con el fin de proponer los lineamientos para la construcción de un software, apoyándose en diferentes fuentes bibliográficas: eventos relacionados con la temática, revistas, conferencias y repositorios de universidades.

La mayor parte del trabajo se centra en el levantamiento de requisitos o análisis de cada uno de los procesos descritos en Ecu@risk, los mismos que serán modelados utilizando las buenas prácticas de la ingeniería de software, considerando aspectos de calidad, gestión de riesgos y gestión de proyectos.

UNIVERSIDAD DEL AZUAY

2.9 Alcances y resultados esperados:

Contar con un documento que sirva como insumo para el desarrollo de uno de los capítulos del libro "Gestión del riesgo: Una metodología para la gestión de riesgo de información aplicada a las MPYMES" que forma parte de los proyectos de investigación que se lleva en la Universidad del Azuay.

2.10 Supuestos y riesgos:

Supuesto	Probabilidad	Alternativas de solución
Complejidad de la metodología Ecu@Risk.	Media/Alta	Pedir asesoría y entrevistas a expertos en el tema.

2.11 Esquema tentativo:

Capítulo 1: Fundamentación teórica.

Capítulo 2: Análisis de la metodología Ecu@Risk.

Capítulo 3: Identificación de requerimientos.

Capítulo 4: Diseño de software.

- Diagramación de clases
- Casos de uso
- Diagramas de estado
- Diagramas de secuencia
- Diagramas de bases de datos

- Interfaces

Capítulo 5: Gestión de proyecto.

- Identificación de la metodología de gestión de proyectos a utilizar (Tradicionales o Ágiles)
- Acuerdo de proyecto
- Identificación de recursos
- Asignación de tareas
- Calendarización de las tareas y responsabilidades
- Gestión de la calidad
- Estándar de documentación del proyecto

Capítulo 6: Estudio económico

- Presupuesto de desarrollo

Capítulo 7: Gestión de riesgos del proyecto.

- Riesgos de conceptualización
- Riesgos de recursos
- Riesgos financieros

Capítulo 8: Desarrollo del prototipo

Conclusiones y trabajos futuros.

Bibliografía.

2.12 Cronograma:

CRONOGRAMA																								
OBJETIVOS	ACTIVIDADES	Semanas																						
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Fundamentar teóricamente los componentes que permiten el análisis y desarrollo de software bajo principios de ingeniería y buenas prácticas de aseguramiento y calidad.	Fundamentación teórica																							
	Análisis de la metodología Ecu@Risk																							
Proponer directrices para levantamiento de requisitos, y el modelamiento del software.	Análisis comparativo de software para la gestión de riesgos																							
	Identificación de requisitos																							
	Diseño de software																							
	Desarrollo de prototipo																							
Proponer directrices para la gestión del proyecto, contemplando los riesgos que pueden presentarse durante el desarrollo del software para gestión de riesgos de información.	Gestión del proyecto																							
	Estudio Económico																							
	Gestión de riesgos del proyecto																							

2.13 Referencias:

Abril, A., Pulido, J., & Bohada, J. (2013). Análisis de riesgos en seguridad de la información. *Revista Ciencia, Innovación y Tecnología (RCIYT)*, 39-53.

Carranza, P. (2016). Gestión en proyectos de software. *Tecnología, Investigación y Academia, TIA 4(2)*, 12-19.

Crespo, E. (2016). ECU@Risk Una metodología para la gestión de riesgo aplicada a las MPYMES del Ecuador. Cuenca, Azuay, Ecuador.

Delgado, J. (2014). Ciberseguridad en Gobernanza de Internet en Ecuador: Infraestructura y acceso. *Encuentro Nacional de Gobernanza de Internet, Quito, Ecuador.* Quito.

Mascheroni, M., Greiner , R., Petris, R., Dapozo, G., & Estayno, M. (2012). Calidad de software e Ingeniería de Usabilidad. *XIV Workshop de Investigadores en Ciencias de la ComputaciónXIV Workshop de Investigadores en Ciencias de la Computación*, (págs. 656-659). Posadas.

Montoya, M., Pulgarín, E., & Monsalve, J. C. (2014). Estratégias didácticas en el aprendizaje para el levantamiento de requerimientos. En A. S. Arango, *La investigación, un compromiso con la sociedad* (págs. 393-400). Medellín: Fondo Editorial Luis Amigó.

Osorio, N., & Castro, G. (2011). Gestión de calidad en desarrollo de software. *Revista de Investigación de Sistemas e Informática*, 65-69.

Pérez, O., & Zulueta, Y. (2013). Proceso para gestionar riesgos en proyectos de desarrollo de software. *Revista Cubana de Ciencias Informáticas, Vol. 7, No. 2*, 206-221.

Vidal, C., Schmal, R., Rivero, S., & Villaroel, R. (2012). Extensión del Diagrama de Secuencias UML (Lenguaje de Modelado Unificado) para el Modelado Orientado a Aspectos. *Información Tecnológica*, 51-62.

UNIVERSIDAD DEL AZUAY

2.14 Anexos

2.15 Firma de responsabilidad (estudiante)

Pablo Cevallos

2.16 Firma de responsabilidad (director sugerido)

Ing. Esteban Crespo

2.17 Firma de responsabilidad (asesor metodológico)

PhD. Francisco Salgado

2.18 Fecha de entrega: 16 de mayo de 2017

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 Nº 0797229