Universidad de Cienfuegos “Carlos Rafael Rodríguez”
Facultad de Ingeniería
Carrera de Ingeniería Informática

“Trabajo de diploma para optar por el título de Ingeniería en Informática”

Título: “*Sistema informático para la gestión del plan de seguridad informática en la Universidad de Cienfuegos*”

Autor (a):
Omar Alejandro Valladares González

Tutor (a):
Lic. Amanda Riverol Quesada

Cienfuegos, Cuba
Curso 2017 - 2018

Declaración de autoría

Declaro que soy el único autor de este trabajo y autorizo al Departamento de Ingeniería de la Universidad de Cienfuegos y la Facultad de Informática que hagan el uso que estimen pertinente con el trabajo de diploma.

Para que así conste firmo (firmamos) la presente a los ____días del mes de ___ del ___.

	(Si procede)
_____	_____
Nombre completo del primer autor	Nombre completo del segundo autor
	(Si procede)
_____	_____
Nombre completo del primer tutor	Nombre completo del segundo tutor

Los abajo firmantes certificamos que el presente trabajo ha sido revisado según acuerdo de la dirección de nuestro centro y el mismo cumple los requisitos que debe tener un trabajo de esta envergadura referente a la temática señalada.

---	---
Firma Tutor	Firma Tutor
---	---
Firma ICT	Firma Vicedecano

Pensamiento

"Sin una meta final tampoco puede haber metas o medios menores". Solamente una meta final, un fin en sí mismo hace posible la existencia de valores."

Ayn Rand

Agradecimientos

Agradezco a todos los profesores que en el transcurso de estos años han inculcado en mí tanta sabiduría.

A los que desinteresadamente me ayudaron en la preparación y culminación de este trabajo.

A mis compañeros que me dieron ánimos.

A las amistades y familia que me dieron las fuerzas y deseos para culminar mi proyecto y que se mantuvieron siempre dispuestos en los momentos más difíciles para brindarme su abrigo con la mejor de las sonrisas….

A todos,

¨Mil gracias¨

Dedicatoria

A mamá Miriam.

Resumen

El presente trabajo se realizó en la Universidad de Cienfuegos y tiene como objetivo desarrollar una aplicación web para la gestión del plan de seguridad informática en la misma, que contribuya a la elaboración del plan de seguridad informática, a partir de los resultados obtenidos con la realización de una matriz de riesgos. El sistema propuesto facilitará la gestión de manera eficiente de la información para la elaboración del plan de seguridad informática en la Universidad de Cienfuegos. Para llevar a cabo la documentación del negocio, diseño e implementación del sistema se utilizó el Lenguaje Unificado de Modelado (UML), siguiendo lo establecido por la metodología de desarrollo RUP, como gestor de bases de datos se utilizó PosgreSQL, como lenguaje de programación Web se utilizó PHP y el framework Yii, como servidor Web, Apache. El software diseñado cumple con las necesidades reales de los clientes y usuarios finales. El mismo fue sometido a un proceso de validación a través de pruebas funcionales y la justificación de su desarrollo se concretó a partir de un estudio de factibilidad basado en puntos de caso de uso.

Palabras claves: gestión, software, SIGSI, seguridad informática, plan de seguridad.

Abstract

The present work was carried out at the University of Cienfuegos and its objective is to develop a web application for the management of the computer security plan in the same, which contributes to the development of the computer security plan, based on the results obtained with the realization of a risk matrix. The proposed system will facilitate the efficient management of information for the development of the computer security plan at the University of Cienfuegos. To carry out the business documentation, design and implementation of the system, the Unified Modeling Language (UML) was used, following the established by the RUP development methodology, as a database manager, PosgreSQL was used as a web programming language. PHP and the Yii framework were used as Web server, Apache. The software designed meets the real needs of customers and end users. It was subjected to a validation process through functional tests and the justification for its development was made based on a feasibility study based on use case points.

Keywords: management, software, SIGSI, computer security, security plan.

Índice

Índice de tablas

Índice de figuras

Introducción

Introducción

La información es hoy en día uno de los activos más importantes de las organizaciones, y debe protegerse, por ello en la actualidad las empresas y organizaciones utilizan para la creación, procesamiento, transmisión y almacenamiento de su información las ventajas de las Tecnologías de la Información y las Comunicaciones. Debido a esto, el número de amenazas se incrementa y obliga, a que garantizar la disponibilidad, confidencialidad e integridad de la información signifique un aspecto de primer orden, sobre el cual invertir para evitar la pérdida, modificación o robo de los activos informáticos. Antiguamente todo era soporte papel y la seguridad principalmente física. Actualmente lo primordial es el soporte informático y la seguridad lógica.

Los trascendentales cambios operados en el mundo moderno, caracterizado por su incesante desarrollo; la acelerada globalización de la economía, la acentuada dependencia que incorpora un alto volumen de información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, imponen nuevos retos a la práctica de la profesión de auditoría, en particular a la auditoría de seguridad Informática

Cuba realiza grandes esfuerzos e invierte considerables recursos para llevar la informatización a todos los niveles de la sociedad, con el objetivo de mejorar la rapidez del acceso a la información y su organización de una manera adecuada, además, de garantizar la preparación. Producto a los avances alcanzados en los últimos años, con el incremento del uso de tecnologías de la información en todos los sectores; en particular de las redes informáticas y sus servicios asociados, surge como una necesidad del Estado cubano la creación de la Oficina de Seguridad para las Redes Informáticas (OSRI), creada por el Acuerdo 3736/2000 del Comité Ejecutivo del Consejo de Ministros (CECM), adscripta al Ministerio de la Informática y las Comunicaciones (MIC), con el objetivo de prevenir, evaluar, investigar y dar respuesta a las acciones tanto internas como externas que afecten el normal funcionamiento de las Tecnología de la Informática y las Comunicaciones (TIC) en el país.[1]

El proceso de informatización de la sociedad y en particular el de las instituciones cubanas, tiene que ser intrínsecamente seguro. Resulta una necesidad reconocida por todos continuar desarrollando la informatización del sistema de seguridad informática de

la Universidad de Cienfuegos, pero al mismo tiempo se tiene que trabajar en minimizar los problemas existentes en cuanto a la seguridad informática para no comprometer la informatización y, en general, el desarrollo de la educación superior en el país.

La cantidad de incidentes reportados por la OSRI sobre el sistema de seguridad informática de la Universidad de Cienfuegos crece en los últimos años. De acuerdo a sus estadísticas en el 2015 las instituciones del Ministerio de Educación Superior ocuparon el 7mo lugar entre las redes nacionales con mayor número de vulnerabilidades identificadas. Ese mismo año 5 redes del ministerio fueron controladas por la OSRI, obteniéndose en dos de los casos resultados negativos (Muy Vulnerable y Vulnerable).

Estos indicadores se han modificado en lo que va de año pero persiste la detección de incidentes y de vulnerabilidades similares, lo cual indica que los avances en este tema son insuficiente. Esta situación merece una atención especializada, pues en las condiciones de aumento de visibilidad, de intercambio de contenidos significa un crecimiento exponencial de los riesgos.

En varios análisis en el Consejo de Dirección se puso de manifiesto el uso de sistemas de gestión como SIGENU y ASSET por parte de los infractores, sin que su actividad haya sido detectada por esa vía. Generalmente no existen desarrolladores de software en los equipos de administración de redes que se encarguen de gestionar la seguridad informática en esas tareas.

Los especialistas o asesores de seguridad informática, como contraparte a la actividad TIC, son inestables o carecen de la preparación que se requiere. Cuando se introducen nuevos servicios o contenidos en la red, se producen cambios tecnológicos o de infraestructura, que se necesita tener en cuenta en la gestión de seguridad informática, provocando que el proceso sea dinámico y en estos momentos se hace de manera estática lo que conduce a que el plan de seguridad informática no constituya el instrumento que conduce la actividad.

La mayor parte de los usuarios desconocen el uso correcto de los servicios y recursos TIC, lo cual implica debilidad en el eslabón más importante. Este problema de capacitación se extiende a los especialistas.

Introducción

La resolución 127/2007 es el reglamento de Seguridad para las Tecnologías de la Información, donde en su artículo plantea: "El diseño del Sistema de Seguridad Informática y la elaboración del Plan de Seguridad Informática de cada entidad se realizarán en correspondencia con las metodologías establecidas al respecto por la Oficina de Seguridad para las Redes Informáticas, adscripta al Ministerio de la Informática y las Comunicaciones".

Para entender el proceso de gestión de la seguridad informática se debe partir entendiendo que los datos son la representación simbólica, bien sea mediante números o letras de una recopilación de información la cual puede ser cualitativa o cuantitativa, que facilitan la deducción de una investigación o un hecho, por sí solos no aportan ninguna información importante. Dado este concepto se puede llegar entonces a que la información está definida como una serie de datos con significado, que organiza el pensamiento de los seres vivos, en especial el de los seres humanos. En sentido general, la información es un grupo organizado de datos procesados que integran un mensaje sobre un determinado ente o fenómeno; permitiendo que el hombre adquiera el conocimiento necesario para la toma de decisiones en su vida cotidiana.

El Decreto - Ley 199/99 sobre la Seguridad y Protección de la Información Oficial que tiene como objeto, establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial, cuyas normas deben cumplimentar tanto los órganos, organismos, entidades o cualquier otra persona natural o jurídica residente en el territorio nacional, como las representaciones cubanas en el exterior.

La información oficial es aquella que posee un organismo, órgano, entidad u otra persona jurídica o una persona natural, capaz de proporcionar directa o indirectamente datos o conocimientos que reflejen alguna actividad del estado o reconocida por este, y que pueda darse a conocer de cualquier forma perceptible por vista, al oído o al tacto (Artículo no. 5). A los fines de establecer las medidas para su seguridad y protección, se divide en tres grupos:

- **Clasificada:** Esta información es de acceso restringido a la cual solo accede personal interno autorizado.
- **Restringida:** El acceso es de manera restringida solo a personal interno de un área.

- **Limitada:** El acceso es controlado donde solo accede personal interno, público o externo con permiso.

La seguridad informática tiene como objetivo garantizar las condiciones y características de los datos e información. Para llevar a cabo este proceso se debe realizar un análisis de riesgos el cual debe proporcionar:

- Una detallada caracterización del sistema informático objeto de protección.
- La creación de un inventario de bienes informáticos a proteger.
- La evaluación de los bienes informáticos a proteger en orden de su importancia para la organización.
- La identificación y evaluación de amenazas y vulnerabilidades.
- La estimación de la relación importancia - riesgo asociada a cada bien informático (peso de riesgo).

Lo más importante que no debe faltar en la gestión informática, una vez realizado el análisis de riesgos, es el resultado del mismo resumido en:

- ¿Cuáles son los bienes informáticos más importantes a proteger?
- Las amenazas más importantes a considerar de acuerdo al impacto que pudieran tener sobre la empresa.
- Las áreas sometidas a un mayor peso de riesgo, y las amenazas que lo motivan.

Este proceso de gestión se hace de manera manual trayendo consigo demora en la elaboración del plan de seguridad informática, falta de información y de confiabilidad en la misma. Esta insuficiencia en el proceso evidencia una problemática que aún no se aborda de manera completa y justifica el siguiente **planteamiento de investigación**: En la Universidad de Cienfuegos se gestiona la información para la elaboración del plan de Seguridad Informática de manera ineficiente haciéndolo un proceso lento y engorroso.

El **objeto de estudio:** El proceso de confección del plan de seguridad informática, siendo el **campo de acción:** La gestión del plan de seguridad informática en la Universidad de Cienfuegos.

Con este trabajo la **idea a defender** es que el desarrollo de un sistema informático agilizará el control y gestión de la información disminuyendo en gran manera el tiempo requerido para la elaboración del plan de seguridad informática en la Universidad de Cienfuegos.

Partiendo del problema planteado se formula el **objetivo general** del trabajo:
Gestionar el plan de seguridad informática en la Universidad de Cienfuegos mediante un sistema informático.

Objetivos Específicos

- Analizar el proceso de gestión de la seguridad informática para las tecnologías de la información en la Universidad de Cienfuegos.
- Modelar los procesos del negocio y el sistema
- Diseñar el sistema informático que permita gestionar la seguridad Informática en la Universidad de Cienfuegos.
- Implementar el sistema informático que permita gestionar la seguridad Informática en la Universidad de Cienfuegos.
- Validar el sistema.

Tareas desarrolladas para cumplir los objetivos.

- Estudio de las particularidades de la gestión de la seguridad informática.
- Entrevista a los trabajadores de la red, los jefes de áreas y el asesor de seguridad informática de Cienfuegos.
- Estudio de las aplicaciones existentes relacionadas con el problema a resolver.
- Selección de las herramientas, metodologías, lenguajes y tecnologías.
- Diseño de una arquitectura.
- Diseño de la interfaz gráfica de la aplicación.
- Implementación del diseño propuesto.
- Determinación de la factibilidad del proyecto.
- Diseño de los casos de pruebas funcionales del sistema.

Como **aporte práctico** se puede decir que la implementación del sistema informático para la gestión del plan de la seguridad informática permite la existencia de una herramienta para controlar los procesos necesarios para su elaboración.

Introducción

Capítulo I: En este capítulo se abordan aspectos teóricos del tema en análisis, se detallan los conceptos fundamentales y los sistemas ya existentes asociados al mismo, describiendo sus principales características. Se analizan los procesos que están vinculados al objeto de estudio y se definen las técnicas, metodologías y herramientas a utilizar en la elaboración del sistema informático.

Capítulo II: Descripción y construcción de la solución propuesta. Se detallan los artefactos tanto del negocio como del sistema, se especifican los requisitos funcionales y no funcionales del software. Son realizados los diagramas de clases web a implementar. Es diseñado el modelo lógico y físico de base de datos para la manipulación de los datos.

Capítulo III: Estudio de factibilidad y diseño de casos de prueba funcional: En este capítulo se realiza un estudio de la factibilidad de la aplicación que se propone, teniendo en cuenta el análisis de los costos, beneficios y planificación para el desarrollo del mismo. Además, se diseñan los casos de prueba funcional para el sistema y se define la forma de verificar su correcto funcionamiento.

Capítulo 1 Fundamentos teóricos

La seguridad informática como concepto ha venido evolucionando a lo largo del tiempo. Inicialmente fue una disciplina dominada por la élite de los profesionales especializados en el tema, dejando generalmente fuera al individuo e incluso a la organización.

Desde comienzos del presente siglo se propone una visión más abarcadora de la seguridad de la información, que vincula de manera formal elementos como la tecnología, el individuo y la organización, enfatizando en el estudio de éstos y sus relaciones, para repensar la seguridad informática más allá de la experiencia tecnológica tradicional [2]

La seguridad informática o seguridad de la información, es la preservación de la confidencialidad, integridad y disponibilidad de la información. Esto se logra mediante la implantación de un grupo de controles que incluyen políticas, procedimientos, estructuras organizativas y sistemas de hardware y software [3].

La seguridad de la información no es un estado que se alcanza en determinado instante de tiempo y permanece invariable, sino que es un proceso continuo que necesita ser gestionado.

1.1 Gestión de la Seguridad Informática

El proceso de gestión de la seguridad informática se encuentra descrito en el estándar ISO/IEC 27001, el cual constituye una norma certificable a nivel internacional. Esta norma ofrece un modelo para el diseño, implementación, operación, monitorización, revisión y mejora continua de un sistema de gestión de la seguridad de la información (SGSI)[3].

En [4]se plantea la utilización del modelo PDCA (Plan - planificar, Do - hacer, Check – verificar, Act - actuar) para llevar a cabo estos objetivos, donde es necesario realizar las siguientes acciones en cada fase:

- **Planificar:** establecer las políticas, los objetivos, procesos y procedimientos de seguridad informática pertinentes para gestionar los riesgos y mejorar la seguridad de la información, en concordancia con las políticas y objetivos globales de la organización. En esta etapa se realiza el análisis de riesgos y se seleccionan los controles que garantizarán la seguridad informática.

- **Hacer**: implementar y operar las políticas, controles, procesos y procedimientos establecidos.
- **Verificar**: evaluar y medir el desempeño del sistema de seguridad informática contra las políticas y los objetivos de seguridad establecidos, así como revisar la experiencia práctica adquirida, reportando los resultados a la máxima dirección para su revisión.
- **Actuar**: emprender acciones correctivas y preventivas basadas en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del sistema de seguridad informática.

Para cumplir estas fases, es necesario un conjunto de factores y condiciones tales como:

- Apoyo incondicional por parte de la dirección general.
- Alineación de los objetivos de seguridad con los objetivos de la organización.
- Conocimiento de los requerimientos de seguridad.
- Conocimiento de los riesgos.
- Canales de comunicación con los empleados para dar a conocer los aspectos de seguridad.
- Procedimientos de seguridad.

Corti, Betarte & De la Fuente (2005) [5] en su artículo denominado "Hacia una implementación exitosa de un SGSI" citado por Pallas Mega (2009) establecen un mapeo de las etapas del ciclo de Deming y los productos o entregables exigidos por la norma. Los principales procesos por etapas que indica la norma mapeados con las etapas del ciclo PHVA son:[6]

- **Planear (Plan)**
    - Establecer el contexto.
    - Alcance y Límites.
    - Definir Política del SGSI.
    - Definir Enfoque de Evaluación de Riesgos.
    - Identificación de riesgos.
    - Análisis y Evaluación de riesgos.
    - Evaluar alternativas para el Plan de tratamiento de riesgos.

- Aceptación de riesgos.
- Declaración de Aplicabilidad.

- **Hacer (*Do*)**
  - Implementar plan de tratamiento de riesgos.
  - Implementar los controles seleccionados.
  - Definir las métricas.
  - Implementar programas de formación y sensibilización.
  - Gestionar la operación del SGSI.
  - Gestionar recursos.
  - Implementar procedimientos y controles para la gestión de incidentes de seguridad.
- **Verificar (Check)**
  - Ejecutar procedimientos de seguimiento y revisión de controles.
  - Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI.
  - Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad.
  - Revisión de la evaluación de riesgos periódicamente.
  - Realizar auditorías internas.
  - Revisión de alcance y líneas de mejoras del SGSI por la Dirección.
  - Actualizar los planes de seguridad.
  - Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI.
- **Actuar (*Act*)**
  - Implementar las mejoras identificadas para el SGSI.
  - Implementar las acciones correctivas y preventivas pertinentes.
  - Comunicar acciones y mejoras a todas las partes involucradas.
  - Asegurarse que las mejoras logren los objetivos previstos.

En investigaciones realizadas se considera el tema de la seguridad informática como una disciplina del conocimiento donde se busca cerrar la brecha de los eventos

inesperados que puedan comprometer los activos de una organización y así contar con estrategias para avanzar ante cualquier eventualidad [7].

La creciente cantidad de amenazas que sufren las organizaciones al interior y exterior de los sistemas de información, hace que crezca la necesidad de gestionar de manera eficiente los riesgos.

Dentro del tema de análisis de riesgo se ven reflejados cinco elementos muy importantes dentro del concepto estos son los siguientes: probabilidad, amenazas, vulnerabilidades, activos e impactos.

1.1.1 Análisis de riesgo

El análisis de riesgo es el proceso cuantitativo o cualitativo que permite evaluar los riesgos. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente. Los resultados obtenidos del análisis, van a permitir aplicar alguno de los métodos para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlos, preparar planes para este tratamiento y ejecutarlos.

1.1.1.1 Metodología para el análisis de riesgos

El hecho de conocer los marcos de referencias para el análisis de riesgo no asegura que el proceso se lleve a cabo en forma exitosa. Es por esto que se requiere adicionalmente de una metodología que, en forma eficaz y eficiente, aplique los marcos de referencias exitosamente.

La metodología **MAGERIT** establece como realizar el análisis y gestión de riesgos. Propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, se identifican las amenazas y se determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados. [8]

Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

OCTAVE (OperationallyCriticalThreat, Asset and VulnerabilityEvaluation) [9]es una metodología desarrollada por el CERT/CC2 [10][11] que tiene por objeto facilitar la

evaluación de riesgos en una organización. Se centra en el estudio de riesgos organizacionales[12] y se focaliza principalmente en los aspectos relacionados con el día a día de las empresas.

- La evaluación inicia a partir de la identificación de los activos relacionados con la información, (sistemas de información, software, archivos físicos o magnéticos, personas, entre otros).
- El estudio es desarrollado por un equipo interdisciplinario llamado *el equipo de análisis*, el cual se compone de personas de las áreas de negocio (son los más indicados para identificar qué información es importante en los procesos del día a día y cómo se usa dicha información) y del área de tecnología (son las personas que conocen los detalles de configuración de la infraestructura y las debilidades que puede tener).

El equipo de análisis debe:

- Identificar los activos relacionados con la información que son de importancia para la organización.
- Las amenazas a las que están expuestos y las vulnerabilidades (organizacionales y tecnológicas).
- Finalmente, se define una estrategia basada en prácticas para el mejoramiento organizacional y un plan de mitigación para reducir el riesgo al que está expuesta la organización.

En [13]una metodología basada en la integración de varios modelos, normas, herramientas y buenas prácticas para la implementación de la gestión automatizada de controles de seguridad informática, combinando varios métodos dirigidos a la gestión de riesgos con un enfoque de automatización durante las etapas de operación, monitorización y revisión de un SGSI.

1.1.2 Flujo actual de los procesos y análisis crítico de la ejecución de estos

El flujo actual del proceso se hace en tres etapas, la información necesaria para estas etapas se solicita y se recibe mediante un correo:

Etapa 1- En esta etapa se construyen los perfiles de amenazas basados en los activos:

- Los diferentes miembros de las áreas detectan los activos que son críticos, la manera como se usan y lo que en la actualidad se está haciendo para protegerlos.
- El jefe de área evalúa la información y selecciona los activos más importantes.

Etapa 2- Identificar vulnerabilidades en la infraestructura:

Los administradores de red de cada área identifican los diferentes componentes que se relacionan con cada activo crítico y las vulnerabilidades que pudieran facilitar las acciones no autorizadas sobre los activos críticos.

Fase 3- Desarrollar estrategias y planes de seguridad

En esta etapa el asesor de seguridad informática identifica los riesgos sobre los diferentes activos críticos y decide qué acciones tomar. Crea una estrategia de protección y planes de mitigación, basados en la información recolectada.

Los resultados de este proceso son los siguientes productos:

- Activos críticos: Se identifican los activos relacionados con la información que son de mayor criticidad para la operación y subsistencia de la organización.
- Perfiles de amenazas: Un perfil de amenaza es una manera estructurada de mostrar las diferentes amenazas que se presentan sobre cada activo crítico.
- Puntos de inflexión: Se identifican los componentes más importantes que están relacionados con cada activo crítico como firewalls, servidores, routers, sistemas de backup y almacenamiento de información, entre otros; a fin de visualizar todos los caminos de acceso al activo crítico y elementos que se puedan constituir en puntos de acceso no autorizado al activo evaluado.
- Identificación y evaluación de riesgos: Basados en la información de las etapas anteriores y particularmente en los perfiles de amenazas, se identifican los riesgos y se evalúa el impacto en términos de una escala predefinida (alto, medio, bajo) de acuerdo con los criterios que deben definirse durante las fases anteriores. Estos criterios pueden basarse, a su vez, en aspectos como: pérdidas económicas, afectación de la imagen, generación de riesgo sobre vidas humanas, entre otros.
- Medidas de mitigación del riesgo: Se desarrollan las medidas de mejora y los próximos pasos para proteger los activos críticos.

1.1.3 Sistemas existentes para la gestión de la seguridad informática

La gestión de la seguridad informática se realiza para asegurar la información de los niveles adecuados de protección en cuanto a Confidencialidad, Integridad y Disponibilidad. Para lograr esta gestión de manera efectiva es necesario usar la tecnología adecuadamente y explotar todas sus bondades, así como involucrar al personal y capacitarlo para hacerle frente a dichas amenazas. Existen varios sistemas que tratan la gestión de la seguridad informática. Estos sistemas son:

- **Sistema de Gestión de la Seguridad de la Información (SGSI)**: tiene como objetivo principal identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a los procesos y servicios que presta la organización con apoyo de TI, además de verificar la existencia de controles de seguridad que permitan integrarlos a las políticas y procedimientos para mitigar los riesgos encontrados**.**[6]
- **Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín**. Este sistema aborda una investigación realizada en la Universidad de Ciencias Médicas de Holguín, motivada por la necesidad de contar con una herramienta de apoyo para la gestión de reportes de incidentes, control del estado de protección de los medios informáticos, así como la mejor preparación de los trabajadores en aspectos relacionados con la seguridad informática. Tiene como objetivo fundamental la resolución de un conjunto de dificultades en este aspecto, como son los relacionados con la fluidez de la información, la centralización y confiabilidad en sus datos, para mitigar estos perjuicios se desarrolló una herramienta informática que apoya la gestión de la información sobre seguridad informática.[14]

1.2 Metodologías actuales

Rational Unified Process (RUP) es una metodología que tiene como objetivo ordenar y estructurar el desarrollo de software, en la cual se tienen un conjunto de actividades necesarias para transformar los requisitos del usuario en un sistema Software (Amo, Martínez y Segovia, 2005). [15] Inicialmente fue llamada UP (Unified Process) y luego cambió su nombre a RUP por el respaldo de Rational Software de IBM. Ésta

metodología fue lanzada en 1998 teniendo como sus creadores a Ivar Jacobson, Grady Booch y James Rumbaugh. El RUP nació del UML (Unified Modeling Language) y del UP (Sommer- ville, 2005). [16]

Características del RUP

El RUP es un proceso basado en los modelos en Cascada y por Componentes, el cual presenta las siguientes características: Es dirigido por los casos de uso, es centrado en la arquitectura, iterativo e incremental [17], lo cual es fundamental para el proceso de desarrollo de software.[18]

1.2.1 Lenguaje Unificado de Modelado.

UML (Unified Modeling Language) es un lenguaje que permite modelar, construir y documentar los elementos que forman un sistema software orientado a objetos. Se ha convertido en el estándar de la industria, debido a que ha sido impulsado por los autores de los tres métodos más usados de orientación a objetos: Grady Booch, Ivar Jacobson y Jim Rumbaugh. Estos autores fueron contratados por la empresa Rational Software para crear una notación unificada en la que basar la construcción de sus herramientas CASE[19]. Este lenguaje tiene una notación gráfica muy expresiva que permite representar en mayor o menor medida todas las fases de un proyecto informático desde el análisis con los casos de uso, el diseño con los diagramas de clases, objetos, etc., hasta la implementación y configuración con los diagramas de despliegue. [19]

UML es ante todo un lenguaje. Un lenguaje proporciona un vocabulario y unas reglas para permitir una comunicación. En este caso, este lenguaje se centra en la representación gráfica de un sistema. [20]

Los objetivos de UML son muchos, pero se pueden sintetizar sus funciones:

- Visualizar: permite expresar de una forma gráfica un sistema de forma que otro lo puede entender.
- Especificar: permite especificar cuáles son las características de un sistema antes de su construcción.
- Construir: A partir de los modelos especificados se pueden construir los sistemas diseñados.

- Documentar: Los propios elementos gráficos sirven como documentación del sistema desarrollado que pueden servir para su futura revisión.

1.3 Tecnologías actuales.

Las aplicaciones Web interactivas poco a poco han revolucionado la forma de utilizar internet, aumentando el contenido de las páginas con texto a un contenido rico e interactivo, por lo tanto escalable.

Uno de los primeros lenguajes de programación para el desarrollo de aplicaciones web es el "Perl". Fue inventado por Larry Wall en 1987 antes de que internet se convirtiera en accesible para el público en general. Pero fue en 1995 cuando el programador Rasmus Lerdorf puso a disposición el lenguaje PHP con este el desarrollo de aplicaciones web realmente despegó.[21]

El uso de frameworks en la construcción de aplicaciones pequeñas se generó con la “revolución web 2.0″, una compañía de 5 personas lanzó BaseCamp, un servicio de administración de proyectos basado en web y construido sobre Rails, un framework de desarrollo web para el versátil lenguaje “Ruby“. [22]

Un *framework* se emplea en muchos ámbitos del desarrollo de sistemas software, no solo en el ámbito de aplicaciones Web. Se puede encontrar frameworks para el desarrollo de aplicaciones médicas, de visión por computador, para el desarrollo de juegos, entre otros.

En general, el término framework, se refiere a una estructura de software compuesta de componentes personalizables e intercambiables para el desarrollo de una aplicación. Un framework se puede considerar como una aplicación genérica incompleta y configurable a la que se le puede añadir las últimas piezas para construir una aplicación concreta.

Los objetivos principales que persigue un framework son: acelerar el proceso de desarrollo, reutilizar código ya existente y promover buenas prácticas de desarrollo como el uso de patrones.

Un framework Web, se puede definir como un conjunto de componentes (por ejemplo clases en java, descriptores y archivos de configuración enXML) que componen un diseño reutilizable que facilita y agiliza el desarrollo de sistemas Web[23]

1.3.1 Tipos de framework Web.

Existen varios tipos de frameworks Web: orientados a la interfaz de usuario, como Java Server Faces, orientados a aplicaciones de publicación de documentos, como Coocon, orientados a la parte de control de eventos, como Struts y algunos que incluyen varios elementos como Tapestry. En la Tabla 1 se puede ver algunos de los framework que existen.[23]

Nombre del Framework	**Características**
Yii	• Un poco más fácil de aprender que otros framework, cuenta con foro y IRC que proporciona ayuda al usuario. • Se genera código basura y en ocasiones no lo filtra de la mejor forma y complica el uso de este. • Software libre, patrón de diseño modelo vista controlador, integración con JQuery.
CakePHP	• Facilita al usuario la interacción con la base de datos. Contiene componente de seguridad. • Las versiones del framework influyen en las versiones de uso de PHP. • Compatible con PHP 4 y 5, validación integrada, Sintetización de datos.
Laravel	• Además de manejar el MVC también cuenta con el uso de mapeo objeto-relacional. • Es relativamente nuevo y muchos dejan de utilizarlo porque creen que no es confiable. • Administrador de extensiones, completa documentación, contiene ORM.
Symfony	• Fácil de instalar y usar en la mayoría de plataformas, se extender permite una mejor integración de bibliotecas. • No es muy robusto. • Contiene una gran cantidad de plugins, integración con AJAX.

Tabla 1: Frameworks explicados

1.3.2 MySQL

MySQL sistema de gestión de base de datos relacional y multiusuario con más de seis millones de instalaciones. Por un lado, se ofrece bajo la GNU GPL para cualquier uso compatible con esta licencia, pero para aquellas empresas que quieran incorporarlo en productos privativos deben comprar a la empresa una licencia específica que les permita este uso. Está desarrollado en su mayor parte en ANSIC [24]

Al contrario de proyectos como Apache, donde el software es desarrollado por una comunidad pública y el copyright del código está en poder del autor individual, MySQL es propietario y está patrocinado por una empresa privada, que posee el copyright de la mayor parte del código[24] Su popularidad como aplicación web está muy ligada a PHP, que a menudo aparece en combinación con MySQL. Es una base de datos muy rápida en la lectura cuando utiliza el motor no transaccional MyISAM, pero puede provocar problemas de integridad en entornos de alta concurrencia en la modificación. En aplicaciones web hay baja concurrencia en la modificación de datos y en cambio el entorno es intensivo en lectura de datos, lo que hace a MySQL ideal para este tipo de aplicaciones. Sea cual sea el entorno en el que se va a utilizar MySQL, es importante adelantar monitoreos sobre el desempeño para detectar y corregir errores tanto de SQL como de programación [25]

1.3.3 Forma de validar el sistema web

Pruebas funcionales

Una prueba funcional: es una prueba basada en la ejecución, revisión y retroalimentación de las funcionalidades previamente diseñadas para el software. Las pruebas funcionales se hacen mediante el diseño de modelos de prueba que buscan evaluar cada una de las opciones con las que cuenta el paquete informático. Dicho de otro modo son pruebas específicas, concretas y exhaustivas para probar y validar que el software hace lo que debe y sobre todo, lo que se ha especificado**.**[26]

Fases

Las pruebas funcionales se dividen en las siguientes fases:

Análisis de requisitos (Planificación)

En esta fase se inicia la elaboración del modelo jerárquico de requisitos de prueba partiendo de los procesos funcionales que soporta el producto o activo de software a evaluar. A partir de las funcionalidades se elaborará el plan de pruebas. Hay que obtener toda la información posible de las aplicaciones sobre las cuales se realizarán las pruebas. Esta información se deberá conseguir de toda la documentación disponible sobre su funcionamiento y hablando con el personal responsable de la misma.

Diseño del plan de pruebas (Preparación)

En esta fase se identifica, acuerda y especifican los atributos y características de calidad que se van a probar. El objetivo es diseñar las pruebas para que tengan la mayor probabilidad de encontrar defectos con la mínima cantidad de esfuerzo y tiempo. Serán pruebas que se llevarán a cabo a través de la interfaz gráfica del software (GUI). Es decir, demostrar que las funciones del software son operativas, que la entrada se acepta de forma adecuada y que se produce una salida correcta, así como que la integridad de la información externa se mantiene. Se crearán casos de prueba divididos en pasos (steps) para cada acción a realizar con un resultado esperado asociado, que podrá ser verificado. Durante la fase de diseño también se especifican los datos de entrada necesarios para que los casos de pruebas definidos puedan ser ejecutados (ya sea buscando el éxito de la prueba, o bien el fallo).

Ejecución

En esta fase se ejecutarán los casos de prueba anteriormente diseñados de forma manual. Hay que seguir al detalle el guión establecido dejando cierta libertad al tester para detectar situaciones anómalas no contempladas. Las baterías de pruebas serán ejecutadas como mínimo una vez antes del paso a producción, independientemente de las ejecuciones anteriores. Los casos de prueba fallados se reportarán a los desarrolladores para su corrección hasta que su resultado sea correcto.

Gestión de Incidencias (Defectos)

La gestión de incidencias es una parte implícita de la fase de ejecución, pero que al tener una alta importancia en las pruebas funcionales, se diferenció como una etapa independiente. Cuando al realizar la acción de un step el resultado obtenido no es el esperado, habrá que abrir o reportar una incidencia para que el equipo de desarrollo tenga constancia del error. La gestión de incidencias es el principal canal de comunicación con el equipo de desarrollo. Las incidencias han de ser claras y con todo lujo de detalle, tienen que describir el error para que el equipo de desarrollo pueda comprenderlo perfectamente, reproducirlo, localizarlo y poder solucionarlo. Se deberá mantener una continua comunicación con el equipo de desarrollo para conocer el estado de los defectos y poder realizar las repruebas necesarias para su cierre.[27]

1.4 Conclusiones

En este capítulo se abordaron las condiciones y problemas que rodean el objeto de estudio a través de los conceptos y definiciones planteadas y se realizan los siguientes análisis.

- Se analizaron los softwares existentes en el mercado a nivel internacional y nacional.
- Se analizaron la metodología para el desarrollo de software y se decidió tomar la metodología RUP por la envergadura del proyecto y las facilidades que muestra la misma.
- Se analizaron las tecnologías que serán utilizadas en la realización del proyecto, entre ellas están: los lenguajes HTML, CSS y JavaScript. Se utilizará como framework, Yii Framework y para el almacenamiento de los datos se seleccionó MySQL.

Estas metodologías, lenguajes y herramientas fueron evaluados en conjunto con los clientes y se decidió utilizar las mismas por ser las más adecuadas para darle solución a la problemática propuesta.

2 Capítulo 2 Construcción de la solución propuesta

2.1 Modelo del negocio

La presencia de un proceso bien definido y bien gestionado, es fundamental para el entendimiento del problema a resolver. En este capítulo se realizará el análisis y diseño de la solución propuesta, se utilizará como metodología de desarrollo de software RUP, cuyos artefactos serán modelados a partir de la herramienta Visual Paradigm haciendo uso del lenguaje de modelado UML.

Los artefactos a generar como parte del modelado del negocio son: actores y trabajadores del negocio, los casos de uso del negocio y sus descripciones, el diagrama de actividad, reglas del negocio, así como el modelo de objetos.

2.1.1 Descripción del modelo de negocio

El proceso fundamental del negocio es realizar el plan de seguridad informática con el objetivo de facilitar la toma de decisiones con respecto a la seguridad informática de la universidad.

La elaboración del plan de seguridad informática comienza con la solicitud de este por parte de los jefes de áreas. Para dar respuesta a esta solicitud el asesor de seguridad informática elabora el análisis de riesgo, para el cual el asesor de seguridad informática solicita la siguiente información mediante correo electrónico:

- A los administradores de red, la ficha de amenazas, la cual como se observa en el Anexo A1 recoge la información relacionada con las amenazas detectadas especificando el tipo y la probabilidad de ocurrencia.
- A los jefes de áreas, la elaboración de la ficha de datos, la cual como se observa en el Anexo A2 cuenta con dos formularios en los cuales se recogen:
    1. Los datos de la información que manejan los trabajadores de su área, la cual tiene que clasificar en función del acceso a la misma y medir la magnitud del daño que causaría la pérdida de esta.
    2. Los datos de la infraestructura con la que se maneja esta información, clasificar el uso de la misma en función de la cantidad de usuarios que tienen acceso y la magnitud del daño que causaría la pérdida de la misma.

Una vez que el asesor de seguridad informática cuenta con la información, procede a elaborar:

- Una ficha de amenazas general que contiene el conjunto de amenazas establecidas por los administradores de red y le asigna una probabilidad de ocurrencia a cada una. Esta probabilidad coincide con el promedio de las probabilidades establecidas por los administradores de red para la amenaza.
- Una ficha de datos e información general que se maneja en todas las áreas de la universidad relacionada con la infraestructura que la almacena.

Una vez elaboradas estas dos fichas se procede a la elaboración de la matriz de riesgo en un fichero Excel, relacionando la información manejada por las áreas y la infraestructura que la almacena con las amenazas a las que están expuestas, valorando la probabilidad de ocurrencia de las mismas y la magnitud del daño que causaría la pérdida de esta para la institución.

La matriz de riesgo (MR) es una matriz de I filas y A columnas donde I es la cantidad de información que maneja la universidad y A la cantidad de amenazas a las que están expuestas. El valor de la matriz de riesgo se calcula por la ecuación 1 donde MDI_i es la magnitud del daño provocado por el documento *i y* PA_jes la probabilidad que ocurra la amenaza *j*.

$$MR_{ij} = MDI_i * PA_j \quad (1)$$

Con los datos recogidos el asesor de seguridad informática elabora una caracterización de la red en cuanto a los servicios e información que se manejan en la universidad así como la infraestructura y los usuarios.

Basado en esta caracterización y en la matriz de riesgo el asesor de seguridad informática detecta los puntos de inflexión y establece las áreas a proteger.

Finalmente procede con toda esta información a la elaboración de una propuesta del Plan de Seguridad Informática (PSI). En el PSI se establecen medida para prevenir mitigar o evitar los daños. El PSI es analizado en un consejo de dirección por los jefes de áreas los cuales pueden sugerir modificaciones al mismo. Si los jefes de áreas sugieren modificaciones el PSI es adaptado por el asesor de seguridad informática a las sugerencias y es enviado de nuevo para su análisis. El proceso termina cuando todos los jefes de áreas aprueban el plan. El plan de seguridad informática es aplicado por los

jefes de áreas para prevenir, mitigar o evitar los daños en la información manejada por los trabajadores del área.

2.2 Reglas del negocio a considerar

- ✓ Solo el asesor de seguridad informática puede solicitar la elaboración de las fichas.
- ✓ A la información de la ficha general de datos e información solo puede acceder el asesor de seguridad informática.
- ✓ Solo tiene acceso a la ficha de información de cada área el jefe del área y el asesor de seguridad.
- ✓ Todos los elementos de la ficha de datos e información tienen que estar relacionados como mínimo con una infraestructura establecida en la ficha.
- ✓ Los administradores de área tienen que establecer la magnitud del daño causado por cada elemento de la ficha de datos e información.
- ✓ Los administradores de red tienen que establecer la probabilidad de que ocurra cada elemento de la ficha de amenazas.
- ✓ Solo el asesor de seguridad informática puede acceder a la matriz de riesgo.
- ✓ Cada punto de inflexión detectado en la matriz de riesgo tiene que contar con al menos una medida.
- ✓ El plan de seguridad informática no es válido si no está aprobado por todos los administradores de área.
- ✓ Una vez aprobado el plan de seguridad informática no puede ser modificado, en caso de serlo, se convertiría en un plan no válido.

2.3 Modelo de casos de uso del negocio

El modelo de casos de uso del negocio describe los procesos de una empresa en términos de casos de uso y actores del negocio en correspondencia con los procesos del negocio y los clientes, respectivamente. [17]

2.3.1 Actores del negocio

Nombre del actor	Descripción
Jefe de Área	Son los encargados de: Solicitar una propuesta de PSI. Aprobar las medidas propuestas en el plan de seguridad informática elaborado por la asesora de seguridad.

Tabla 2. Descripción de los actores del negocio

2.3.2 Diagramas de casos de uso del negocio

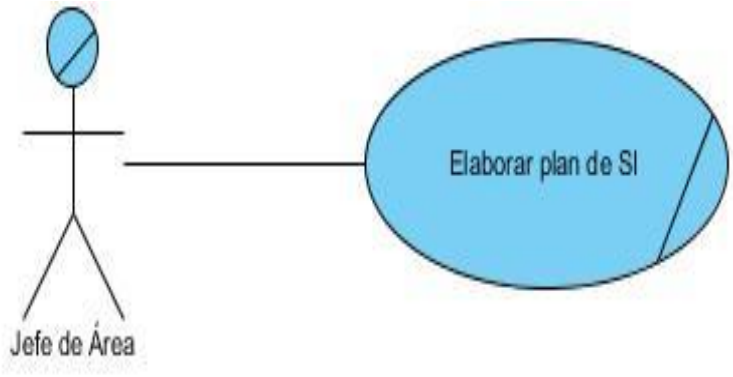


Figura 1: Diagrama de casos de uso del negocio

2.3.3 Trabajadores del negocio

Nombre del trabajador	Descripción
Asesor de Seguridad Informática	Representa a un trabajador que presta sus servicios retribuidos subordinados a la universidad, tiene como responsabilidad elaborar: • Descripción de la red. • La matriz de riesgo. • La propuesta del PSI.

Administrador de red	Representa a un trabajador que presta sus servicios retribuidos subordinados a la universidad, tiene como responsabilidad elaborar la ficha de amenazas y recopilar todos los datos necesarios para la información de los elementos en la ficha.
Jefes de Área	Representa a un trabajador que presta sus servicios retribuidos subordinados a la universidad, tiene como responsabilidad elaborar la ficha de datos e información y recopilar todos los datos necesarios para la información de los elementos en la ficha. Puede además modificar las medidas propuestas en el plan de seguridad informática elaborado por la asesora de seguridad. Son los encargados de aplicar las medidas en el PSI para prevenir mitigar o evitar los daños en la información manejada.

Tabla 3. Descripción de los trabajadores del negocio

2.3.4 Descripción de los casos de uso del negocio

Después de identificar todos los procesos que forman parte del negocio es necesario realizar una explicación más detallada de los mismos. La descripción textual y el diagrama de actividad asociado a cada caso de uso facilitan el entendimiento del proceso.

Caso de Uso del Negocio	**Elaborar plan de SI**
Actores	Jefe de Área(inicia)
Propósito	A partir de un análisis de riesgos se detectan los puntos de

	inflexión para establecer las áreas a proteger y elaborar a la vez una caracterización de la red en cuantos a los servicios e información que se manejan en la universidad así como la infraestructura y los usuarios. Procediendo a la elaboración del Plan de Seguridad Informática.

Resumen

El propósito de este caso de uso es realizar el Plan de Seguridad Informática con el objetivo de facilitar la toma de decisiones con respecto a la seguridad informática de la universidad.

Tiene inicio, cuando los jefes de área realizan una solicitud a la asesora de SI para la realización del plan. Para dar respuesta a esta solicitud el asesor de seguridad informática elabora un análisis de riesgo para el cual solicita mediante correo electrónico información a los propios jefes de área relacionada con los datos de la información que manejan los trabajadores de su área y los datos de la infraestructura con la que se maneja esta información y además al administrador de red solicita información relacionada con las amenazas detectadas especificando el tipo de amenazas y la probabilidad de ocurrencia. Una vez obtenida la información el asesor de seguridad informática elabora una ficha de amenazas general y una ficha de datos e información general. Una vez elaboradas estas dos fichas se procede a la elaboración de la matriz de riesgo, con los datos recogidos el asesor de seguridad informática elabora una caracterización de la red en cuantos a los servicios e información que se manejan en la universidad así como la infraestructura y los usuarios y basado en esta caracterización y en la matriz de riesgo el asesor de seguridad informática detecta los puntos de inflexión y establece las áreas a proteger. Finalmente procede con toda esta información a la elaboración de una propuesta del Plan de Seguridad Informática (PSI).

Curso Normal de los eventos	
Acción del Actor	**Respuesta del negocio**
1- El jefe de área realiza una solicitud a la asesora de SI para la realización del plan de	2-Para dar respuesta a esta solicitud el asesor de seguridad informática solicita a los administradores de red, la elaboración de la ficha de amenazas y a los jefes de áreas, la elaboración de la ficha de datos e información

SI.	
	3-Los jefes de área y el administrador de red completan su ficha correspondiente y se la envían de vuelta a la asesora de SI.
	4-La asesora de SI comprueba que la información ingresada en las fichas no posea errores.
	4.1-En caso de no existir errores el asesor de seguridad informática elabora una ficha de amenazas general y una ficha de datos e información general.
	5-Una vez elaboradas estas dos fichas se procede a la elaboración de la matriz de riesgo relacionando la información manejada por las áreas y la infraestructura que la almacena con las amenazas a las que están expuestas, valorando la probabilidad de ocurrencia de las mismas y la magnitud del daño que causaría la pérdida de la misma para la institución.
	6- Con los datos recogidos el asesor de seguridad informática elabora una caracterización de los elementos de la red en cuantos a los servicios e información que se manejan en la universidad así como la infraestructura y los usuarios.
	7- Basado en esta caracterización y en la matriz de riesgo el asesor de seguridad informática detecta los puntos de inflexión y establece las áreas a proteger.
	8-Luego con toda esta información elabora una propuesta de medidas que es enviada al jefe de área para su revisión
9-El jefe de área analiza la propuesta de medidas.	
9.1-En caso de que el	

jefe de área este de acuerdo con las medidas, se aprueban las mismas y son enviadas de vuelta a la asesora.	
	10-La asesora procede a la elaboración de una propuesta del Plan de Seguridad Informática (PSI), en el cual se establecen medidas para prevenir mitigar o evitar los daños
	11- El PSI es enviado al jefe de área el cual puede sugerir modificaciones al mismo.
12-El jefe de área analiza la propuesta de plan.	
12.1-Si los jefes de áreas están de acuerdo con la propuesta de PSI es aprobado el plan.	
Curso Alternativo de los eventos	
	4.2-En caso de existir errores en alguna de las fichas la Asesora de SI se la envía de vuelta ya sea al administrador de red o a los jefes de Área los cuales tienen que corregir los errores en dichas fichas.
9.2-Si el jefe de área sugiere modificaciones a la propuesta de medidas es adaptado por el asesor de seguridad informática a	

las sugerencias y es enviado de nuevo para su análisis.	
12.2-Si el jefe de área sugiere modificaciones a la propuesta de plan, es adaptado por el asesor de seguridad informática a las sugerencias y es enviado de nuevo para su análisis.	
Prioridad	Alta

Tabla 4. Descripción del caso de uso del negocio

2.3.5 Diagramas de actividades del negocio

Un diagrama de actividad posibilita ver las interacciones entre los actores externos del negocio y los trabajadores internos del negocio. Se usan separadores de línea para representar principalmente trabajadores del negocio. Los flujos del objeto se utilizan para demostrar cómo las entidades de negocio se crean y se utilizan en un flujo. [28]

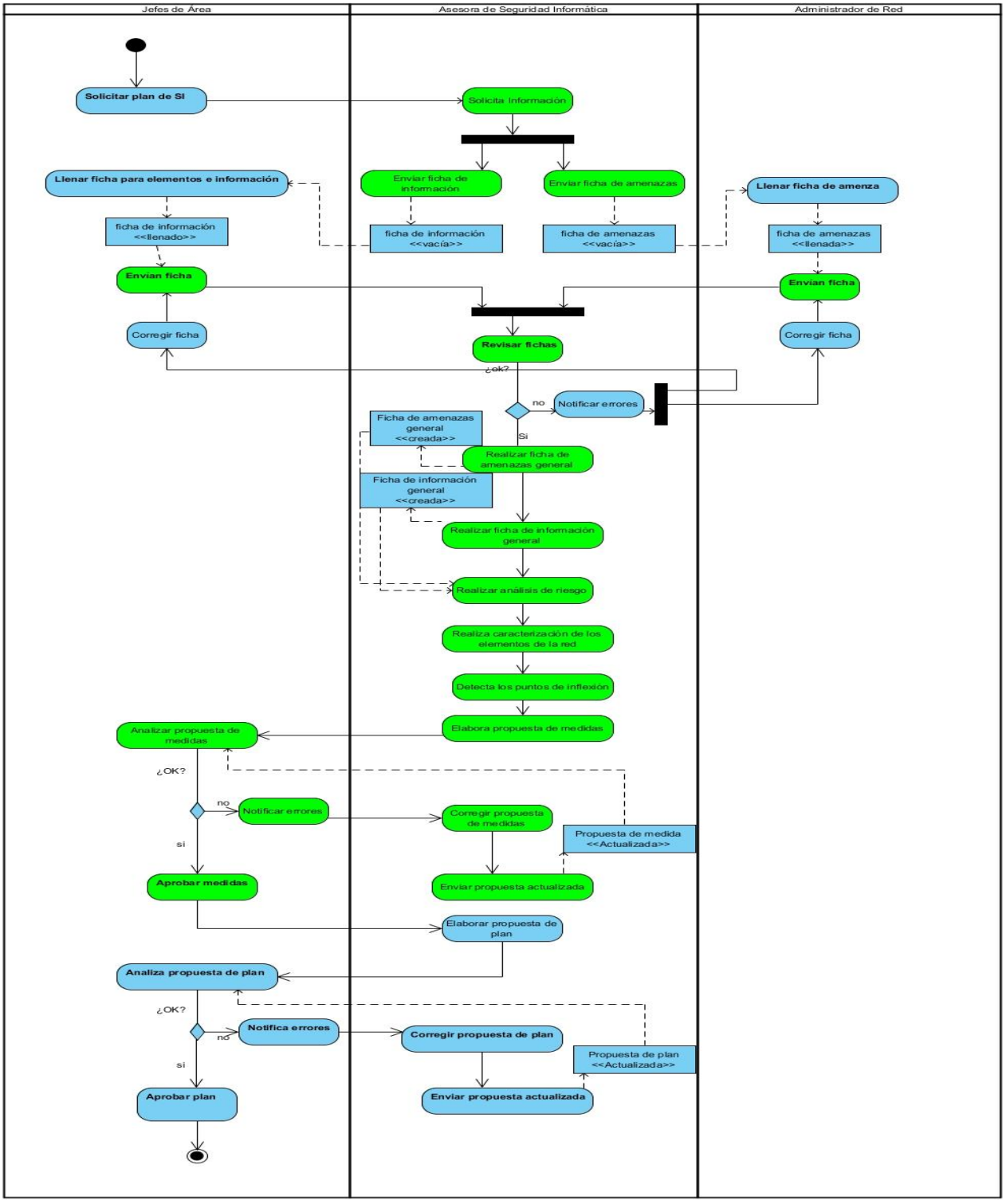


Figura 2. Diagrama de Actividades del caso de uso realizar análisis de riesgo

2.4 Modelo de objetos del negocio

Un modelo de objetos del negocio es un modelo interno a un negocio. Describe como cada caso de uso del negocio es llevado a cabo por parte de un conjunto de trabajadores que utilizan un conjunto de entidades del negocio y unidades de trabajo. Las entidades de negocio representan los objetos que los trabajadores toman, inspeccionan, manipulan, producen o utilizan durante la realización de los casos de uso [29]

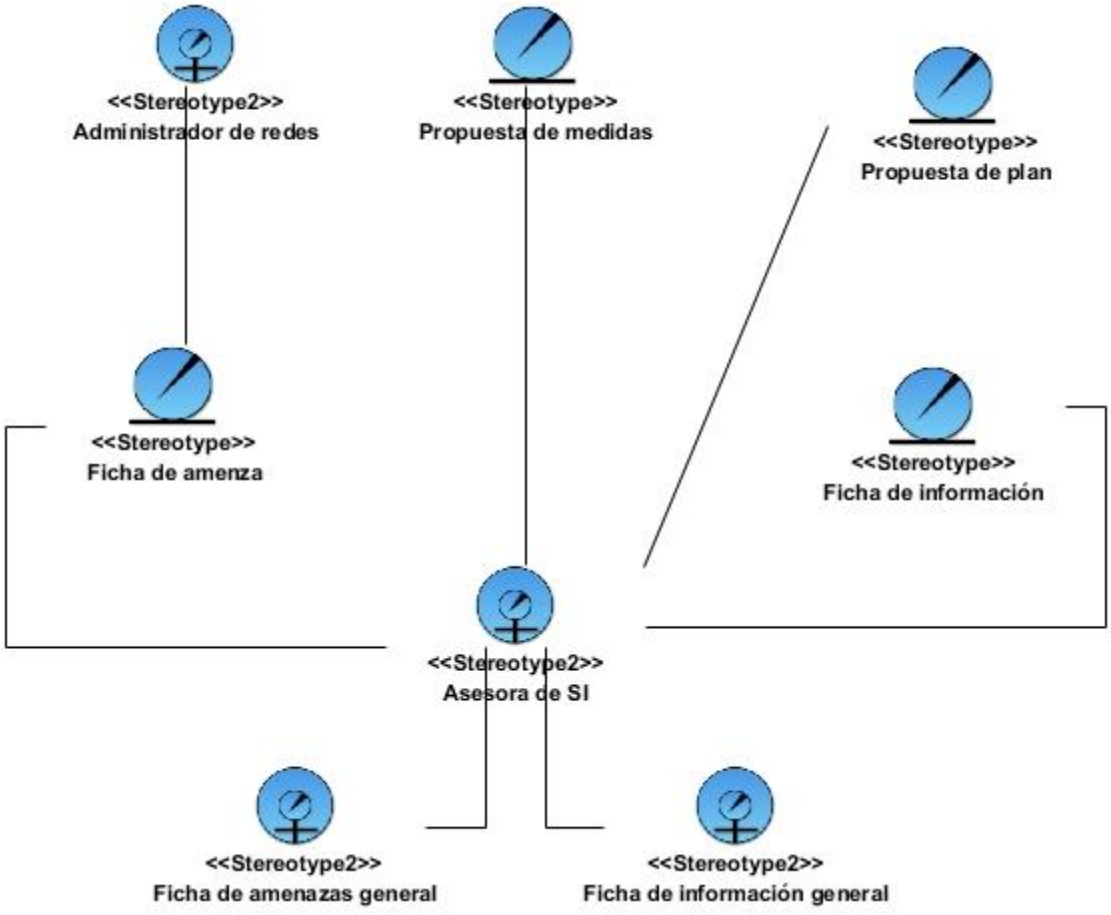


Figura 1.

Figura 3. Diagramas de clases del modelo de objetos del negocio

2.5 Requerimientos

Los requisitos no funcionales especifican propiedades del sistema, como restricciones del entorno o de la implementación, rendimiento, dependencias de la plataforma, factibilidad de mantenimiento, extensibilidad y fiabilidad; con las cuales debe cumplir.

2.5.1 Requerimientos funcionales

1. Autenticarse
2. Cerrar sesión
3. Cambiar contraseña
4. Insertar Usuarios
5. Modificar Usuarios
6. Eliminar Usuarios
7. Listar Usuarios
8. Asignar Rol
9. Insertar datos e información
10. Actualizar datos e información
11. Eliminar datos e información
12. Ver datos e información
13. Insertar infraestructura
14. Modificar infraestructura
15. Eliminar infraestructura
16. Ver infraestructura
17. Relacionar infraestructura con datos e información
18. Insertar datos de Amenaza
19. Actualizar Amenaza
20. Eliminar Amenaza
21. Ver Amenaza
22. Generar descripción de los componentes de la red(reporte)
23. Visualizar descripción de los componentes de la red
24. Visualizar matriz de riesgos
25. Generar matriz de riesgo (reporte)
26. Analizar puntos de inflexión
27. Generar puntos de inflexión(reporte)
28. Relacionar puntos de inflexión con medidas
29. Generar puntos de inflexión con medidas(Reporte)

30. Insertar medidas
31. Modificar medidas
32. Eliminar medidas
33. Ver medidas
34. Aprobar medidas
35. Insertar área
36. Modificar área
37. Ver área
38. Eliminar área

2.5.2 Requerimientos no funcionales

La aplicación diseñada deberá manejar los conceptos conocidos y familiares para los usuarios para que les sea fácil su uso y aprendizaje. Deberá cumplir con los siguientes requisitos no funcionales.

Apariencia o interfaz externa:

La interfaz debe ser diseñada de modo tal que el usuario pueda tener en todo momento el control de la aplicación, lo que le permitirá ir de un punto a otro dentro de ella con gran facilidad. La interfaz debe cumplir con los siguientes requisitos:

- El texto de los mensajes y de la interfaz será en idioma español.
- La ejecución de la aplicación y la introducción de datos deben ser posibles mediante el teclado y el mouse.
- Los mensajes de error serán emitidos desde la aplicación.
- La interfaz debe ser diseñada respetando los parámetros de diseño de la universidad (Colores blanco y azul, logos de la universidad).

Usabilidad: El sistema tiene que ser implementado utilizando tecnología Web permitiendo una fácil manipulación y navegación a los usuarios que tienen acceso a los distintos niveles en los que está estructurado.

Rendimiento: Se concibe un sistema diseñado sobre la arquitectura cliente/servidor, de manera que se pueda contar con varios terminales dentro de la universidad.

Soporte: Se requiere un servidor de bases de datos con soporte para grandes volúmenes de información, velocidad de procesamiento y tiempo de respuesta

rápido en accesos concurrentes. El sistema debe propiciar la anexión de otras opciones que se le incorporen en un futuro.

Seguridad: Se establecerán niveles de privilegio para los diferentes usuarios. El sistema debe ser capaz de restringir el acceso a la información en dependencia del privilegio del usuario.

Software: Para la ejecución del sistema propuesto se necesita tener instalado Internet Information Server (IIS) como servidor Web y SQL Server 2008 R2 como gestor de base de datos. Como sistema operativo Windows 7, 8.0, 8.1, 10 y Framework .NET 4.5. En las computadoras que serán usadas por los usuarios que manipulan la información en el sistema, sólo se requiere de un navegador Web para el acceso al mismo.

Hardware. Para poder utilizar el sistema, se necesita un servidor Web de 1024 Mb de RAM como mínimo, y 2 GB de capacidad del disco duro. Todas las computadoras implicadas, tanto para la administración como para los usuarios, deben estar conectadas a la red y tener al menos 256 Mb de RAM.

2.6 Modelo de casos de uso del sistema

El modelo de casos de uso permite que los desarrolladores del software y los clientes lleguen a un acuerdo sobre los requisitos, es decir, sobre las condiciones y posibilidades que debe cumplir el sistema. Describe lo que hace el sistema para cada tipo de usuario. [17]

Los diagramas de casos de uso se utilizan durante la fase de análisis de un proyecto para identificar y dividir la funcionalidad del sistema. Normalmente contienen: casos de uso, actores y relaciones entre ellos: de asociación, dependencia y generalización.

2.6.1 Actores del sistema

Un actor es aquel que interactúa con el sistema, sin ser parte de él y puede asumir el rol que juega una o varias personas, un equipo o un sistema automatizado [14].

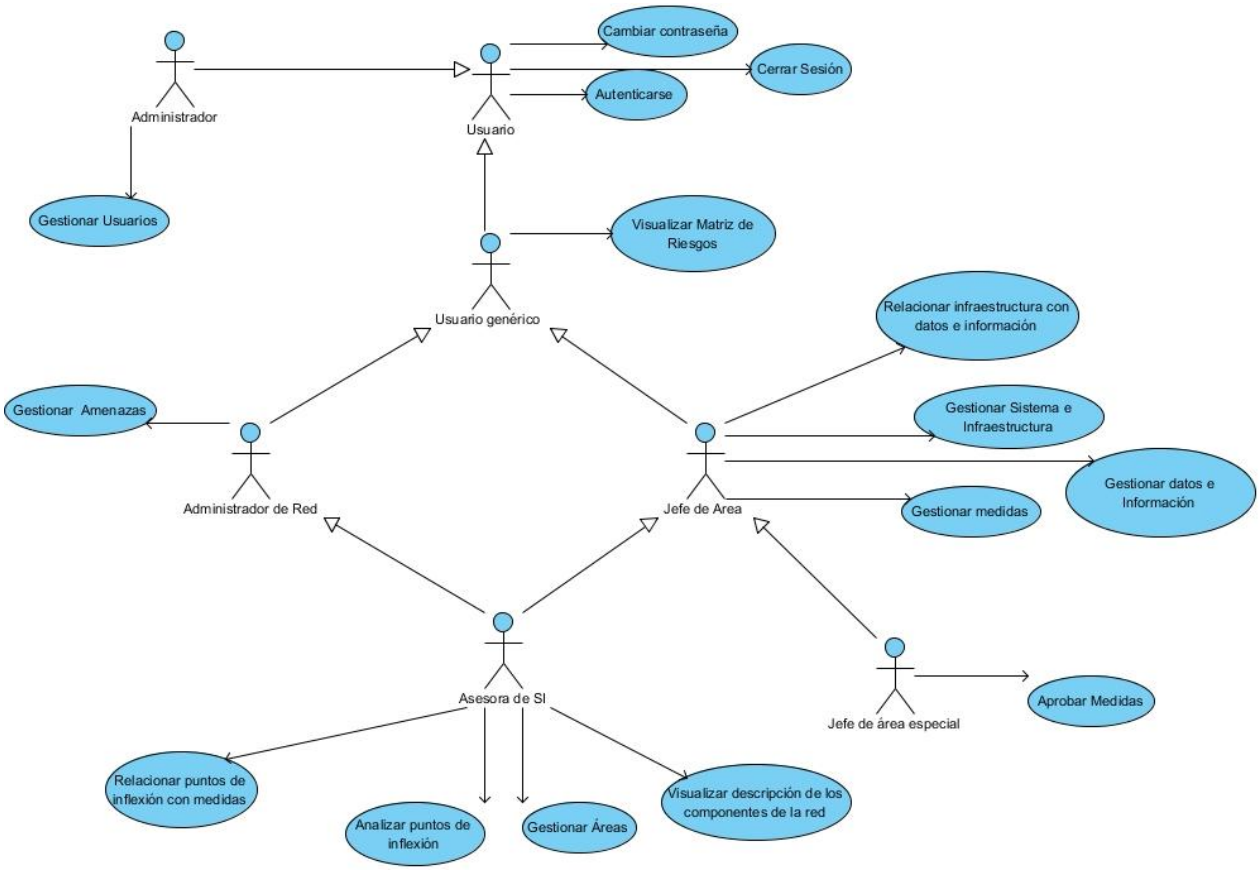
Nombre del actor	Descripción
Usuario	Es todo aquel que puede autenticarse en el sistema, cambiar contraseña, cerrar sesión teniendo en cuenta los requisitos asignados a él.

Administrador	Es el encargado de gestionar los roles y los usuarios en el sistema, ya sea agregar, modificar, editar, o eliminar.
Asesora de SI	Es la encargada de realizar el análisis de riesgo a partir de la información recopilada, además puede analizar los puntos de inflexión obtenidos y relacionarlos con medias, puede gestionar las áreas y además, puede realizar todas las acciones que llevan a cabo los jefes de área y administradores de red.
Jefe de Área	Tiene como responsabilidad enviar información relacionada con las amenazas detectadas especificando ciertos datos de estas como la probabilidad de ocurrencia a partir de la propuesta para el plan que recibe de la asesora de seguridad, elabora el Plan de Seguridad Informática.
Administrador de Red	Tiene como responsabilidad enviar la ficha de elementos para datos e información correspondiente a su área

Tabla 5. Descripción de los actores del sistema

2.6.2 Diagramas de casos de uso del sistema

Para comprender mejor el modelo del sistema, en la figura 5 se muestra el diagrama de casos de uso del sistema.



.

Figura 4Diagramas de casos de uso del sistema

2.6.3 Descripción de los casos de uso del sistema

La descripción de cada caso de uso del sistema puede apreciarse en anexos. La tabla 6 muestra para cada caso de uso el anexo que contiene su descripción.

Caso de Uso	**Descripción**
Autenticarse	Ver Anexo B1
Cerrar sesión	Ver Anexo B2
Cambiar contraseña	Ver Anexo B3
Gestionar usuarios	Ver Anexo B4
Gestionar datos e información	Ver Anexo B5
Gestionar sistema e infraestructura	Ver Anexo B6
Relacionar infraestructura con datos e información	Ver Anexo B7
Gestionar amenazas	Ver Anexo B8
Visualizar descripción de los componentes de la red	Ver Anexo B9
Visualizar matriz de riesgos	Ver Anexo B10

Analizar puntos de inflexión	Ver Anexo B11
Relacionar puntos de inflexión con medidas	Ver Anexo B12
Gestionar medidas.	Ver Anexo B13
Aprobar medidas	Ver Anexo B14
Gestionar áreas	Ver Anexo B15

Tabla 6 Descripción de los Casos de uso del sistema

2.7 Diagramas de diseño de clases web.

Un diagrama de clases de diseño presenta las clases del sistema con sus relaciones estructurales y de herencia correspondientes. En el caso de las aplicaciones web, representa las colaboraciones que ocurren entre las páginas, donde cada página lógica puede ser representada como una clase. [17]

Caso de Uso	**Descripción**
Autenticarse	Ver Anexo C1
Cerrar sesión	Ver Anexo C2
Cambiar contraseña	Ver Anexo C3
Gestionar usuarios	Ver Anexo C4
Gestionar datos e información	Ver Anexo C5
Gestionar sistema e infraestructura	Ver Anexo C6
Relacionar infraestructura con datos e información	Ver Anexo C7
Gestionar amenazas	Ver Anexo C8
Visualizar descripción de los componentes de la red	Ver Anexo C9
Visualizar matriz de riesgos	Ver Anexo C10
Analizar puntos de inflexión	Ver Anexo C11
Relacionar puntos de inflexión con medidas	Ver Anexo C12
Gestionar medidas	Ver Anexo C13
Aprobar medidas	Ver Anexo C14
Gestionar áreas	Ver Anexo C15

Tabla 7: Diagramas de diseño de clases web

2.8 Diseño de la base de datos

En el desarrollo de cualquier sistema informático resulta de vital importancia realizar un buen diseño para el almacenamiento de la información. El sistema maneja información de gran importancia sobre la seguridad informática en la Universidad de Cienfuegos,

por lo que la realización de un buen diseño de la base de datos para poder almacenar la información es imprescindible. A continuación, se muestra el diseño de la base de datos del sistema propuesto a través del modelo lógico y físico de datos.

2.8.1 Modelo lógico de datos.

El modelo lógico de la base de datos determina cómo se estructuran los datos de forma lógica mediante tablas y relaciones. Este diseño puede tener también una gran repercusión en el rendimiento de la aplicación. [17]

Un modelo lógico de datos es un modelo que no es específico de una base de datos que describe aspectos relacionados con las necesidades de una organización para recopilar datos y las relaciones entre estos aspectos. Un modelo lógico contiene representaciones de entidades y atributos, relaciones, identificadores exclusivos, subtipos y restricciones entre relaciones. [30]Ver Anexo D1

2.8.2 Modelo físico de datos.

Un modelo de datos físico es un modelo específico de bases de datos que representa objetos de datos relacionales (por ejemplo, tablas, columnas, claves principales y claves externas) y sus relaciones. [31]Ver Anexo D2.

2.9 Diagrama de despliegue

El modelo físico de datos incluye todos los aspectos de diseño de un modelo de base de datos que se pueden modificar sin cambiar los componentes de la aplicación. [32]

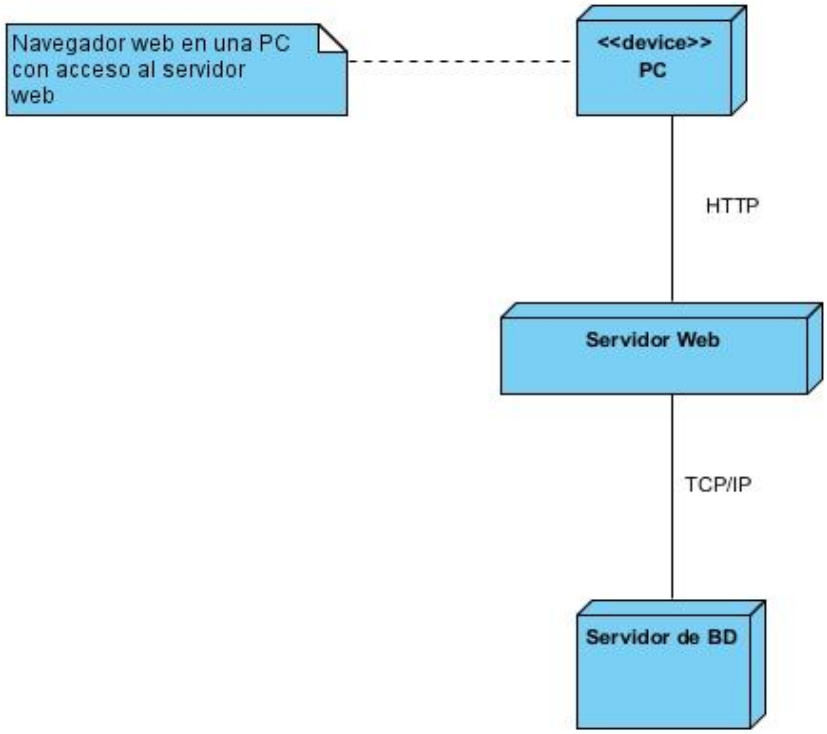


Figura 5. Diagrama de despliegue

2.10 Principios de diseño

El diseño de la interfaz de una aplicación, el formato de los reportes, la concepción de la ayuda y el tratamiento de excepciones tiene gran influencia en el éxito o fracaso de una aplicación. A continuación se describen los principios de diseño seguidos para el desarrollo del sistema en cuestión.

2.10.1 Estándares en la interfaz de la aplicación

Para la creación de la interfaz del sistema se ha utilizado el framework Yii de PHP. Para lograr la apariencia adecuada, se tienen en cuenta varios aspectos, sobre todo relacionados con tipografía, colores, gráficos, navegación, composición del sitio, etc., que a continuación se exponen. En la interfaz diseñada para el sistema se determinó el predominio del color blanco y gris con tonalidades claras y oscuras. La letra que se utiliza es clara con el formato de letra Times New Roman, Monotype Corsiva, y Arial. Se evita el empleo de tantas imágenes para que la aplicación sea lo más rápida posible. El vocabulario manejado es lo menos técnico posible, acercándose al utilizado por los usuarios para obtener un mejor entendimiento y adaptación al sistema. El sistema cuenta con un diseño único, el cual lo integran un menú en la parte superior que permite

al usuario el acceso a todas las funcionalidades en todo momento. La carga visual se distribuye de manera cómoda evitando acumulaciones engorrosas. La entrada de información por parte de los usuarios se realiza a través de los componentes del formulario. Los mensajes de error son pequeños y en español.

2.10.2 Tratamiento de errores

Un papel fundamental en el buen funcionamiento de un sistema informático lo constituye el adecuado tratamiento de errores. El sistema está diseñado para que el usuario escriba solo lo necesario, haciendo uso de listas desplegables con el fin de disminuir el margen de error.

En los formularios se realiza la validación de campos vacíos, para la realización de la operación eliminar se solicita la confirmación del usuario, evitando así posibles errores

2.11 Conclusiones

En este capítulo fueron descritos los procesos fundamentales asociados al modelo del negocio, definiéndose los actores, trabajadores y las reglas que definen el mismo, permitiendo avanzar hacia el modelado del sistema. En el mismo se exponen los requerimientos funcionales y no funcionales del sistema, los actores y los casos de uso que serán implementados posteriormente. Se realizaron además los diagramas de clase web para una mejor comprensión del funcionamiento interno de la aplicación. Se realizados los modelos físico y lógico de la base de datos, y el diagrama de despliegue para definir la organización interna del sistema informático. Posteriormente fueron expuestos los principios de diseños que se tuvieron en consideración, y el tratamiento de errores efectuado en el sistema.

3 Capítulo 3 Estudio de factibilidad.

3.1 Introducción

En el presente capítulo se aborda todo lo referente con la validación y el estudio de factibilidad, mediante las pruebas funcionales, el método de estimación: puntos por casos de uso, la determinación del costo del proyecto, los beneficios tangibles e intangibles y el análisis de costos y beneficios en el desarrollo de la aplicación. Para demostrar si es o no factible el desarrollo del sistema.

3.2 Planificación por casos de usos

3.2.1 Cálculo de los puntos de casos de uso sin ajustar.

UUCP = UAW + UUCW.

UUCP: Puntos de casos de uso sin ajustar.

UAW: Factor de peso de los actores.

UUCW: Factor de peso de los casos de uso.

3.2.2 Factor de peso de los actores sin ajustar (UAW).

Este valor se calcula mediante un análisis de la cantidad de actores presentes en el sistema y la complejidad de cada uno de ellos. La complejidad de los actores se establece teniendo en cuenta en primer lugar si se trata de una persona o de otro sistema, y en segundo lugar, la forma en la que el actor interactúa con el sistema. Los criterios se muestran en la siguiente tabla.

Tipo	**Descripción**	**Peso**
Simple.	Otro sistema que interactúa con el sistema a desarrollar mediante una interfaz de programación. (API, Application Programming Interface).	1
Medio.	Otro sistema que interactúa con el sistema a desarrollar mediante un protocolo o una interfaz basada en texto.	2
Complejo.	Una persona que interactúa con el sistema mediante una interfaz gráfica.	3

Tabla 8 .Factor de peso de los actores del sistema.

Actor	Tipo de actor	Factor de peso
Usuario.	Complejo.	3
Administrador.	Complejo.	3
Asesora de SI	Complejo.	3
Jefe de área	Complejo.	3
Administrador de red	Complejo.	3

Tabla 9 .Forma en que el actor interactúa con el sistema.

Como se describe en la tabla anterior existen en el sistema cinco actores de tipo complejo, debido a que interactúan con el sistema mediante una interfaz gráfica.

Multiplicando la cantidad de actores de cada tipo por el peso correspondiente se obtiene:

UAW = Σ (Actor * Factor de peso) = 15.

3.2.3 Factor de peso de los casos de uso sin ajustar (UUCW)

Este valor se calcula mediante un análisis de la cantidad de casos de uso presentes en el sistema y la complejidad de cada uno de ellos. La complejidad de los casos de uso se establece teniendo en cuenta la cantidad de transacciones efectuadas en el mismo, donde una transacción se entiende como una secuencia de actividades atómica, es decir, se efectúa la secuencia de actividades completa, o no se efectúa ninguna de las actividades de la secuencia. Los criterios se muestran en la siguiente tabla.

Tipo	Descripción	Peso
Simple.	El Caso de Uso contiene de 1 a 3 transacciones.	5
Medio.	El Caso de Uso contiene de 4 a 7 transacciones.	10
Complejo.	El Caso de Uso contiene 8 o más transacciones.	15

Tabla 10 . Factor de peso de los casos de uso del sistema.

Caso de uso	Transacciones	Clasificación
Cambiar contraseña	3	Simple
Cerrar sesión	3	Simple
Autenticarse	3	Simple

Gestionar usuarios	8	Complejo
Visualizar matriz de riesgos	3	Simple
Gestionar amenazas	8	Complejo
Gestionar sistema e infraestructura	8	Complejo
Gestionar datos e información	8	Complejo
Gestionar medidas.	8	Complejo
Relacionar infraestructura con datos e información	3	Simple
Aprobar medidas	8	Complejo
Visualizar descripción de los componentes de la red	3	Simple
Gestionar áreas	8	Complejo
Visualizar puntos de inflexión	3	Simple
Relacionar puntos de inflexión con medidas	3	Simple

Tabla 11. Clasificación de los casos de uso.

Como puede verse en la tabla de clasificación anterior el sistema está conformado por 15 casos de uso de ellos, 8 son simple, y 7 complejos.

De ahí que el factor de peso de los casos de uso sin ajustar puede calcular como:

UUCW = (3*8) + (7*8).

UUCW = 80

Como ya se dispone de los valores de factor de peso de actores y casos de uso sin ajustar, es posible obtener el valor de los puntos de caso de uso sin ajustar:

UUCP = UAW + UUCW

UUCP = 15 + 80

UUCP = 95

3.2.4 Cálculo de los puntos de casos de uso ajustados.

Una vez que se tienen los puntos de casos de uso sin ajustar, se debe ajustar este valor mediante la siguiente ecuación:

UCP = UUCP * TCF * EF.

Donde:

UCP = Puntos de casos de uso ajustados.

UUCP = Puntos de casos de uso sin ajustar.

TCF = Factor de complejidad técnica.

EF = Factor de ambiente.

3.2.5 Factor de complejidad técnica (TCF)

Este coeficiente se calcula mediante la cuantificación de un conjunto de factores que determinan la complejidad técnica del sistema. Cada uno de estos factores se cuantifica con un valor de 0 a 5, donde 0 significa un aporte irrelevante y 5 un aporte muy importante. En la siguiente tabla se muestra el significado, el peso de cada uno, el valor asignado y el total.

Factor	Descripción	Peso	Valor	Pesoi*Valori
T1	Sistema distribuido.	2	3	6
T2	Objetivos de performance o tiempo de respuesta.	1	4	4
T3	Eficiencia del usuario final.	1	3	3
T4	Procesamiento interno complejo.	1	2	2
T5	El código debe ser reutilizable.	1	3	3
T6	Facilidad de instalación.	0.5	3	1.5
T7	Facilidad de uso.	0.5	4	2
T8	Portabilidad.	2	4	8
T9	Facilidad de cambio.	1	3	3
T10	Concurrencia.	1	3	3
T11	Incluye objetivos especiales de seguridad.	1	3	3
T12	Provee acceso directo a terceras partes.	1	3	3

Tabla 12. Factores que determinan la complejidad técnica del sistema

Σ (Pesoi *Valori) = 6+4+3+2+3+1.5+2+8+3+3+3+3+3 = 44.5

El factor de complejidad técnica se calcula mediante la siguiente ecuación.

TCF = 0.6 + 0.01* Σ (Pesoi *Valor asignadoi)
TCF = 0.6 + 0.01 * 44.5
TCF = 1.045

3.2.6 Factor de ambiente (FE):

El Factor de ambiente se calcula atendiendo a las habilidades y el entrenamiento del grupo involucrado. El procedimiento para su cálculo es similar al cálculo del Factor de complejidad técnica.

Factor	**Descripción**	**Peso**	**Valor Asignado**	**Peso$_i$*Valor$_i$**
E1	Familiaridad con el modelo de Proyecto utilizado.	1.5	4	6
E2	Experiencia en la aplicación	0.5	4	2
E3	Experiencia en orientación a objetos.	1	4	4
E4	Capacidad del analista líder.	0.5	4	2
E5	Motivación.	1	5	5
E6	Estabilidad de los requerimientos.	2	4	8
E7	Personal part-time	-1	3	-3
E8	Dificultad del lenguaje de Programación.	-1	3	-3

Tabla 13. Factores que determinan el ambiente.

El factor ambiente se calcula mediante la siguiente ecuación.

Σ (Pesoi * Valori) = 6 + 2 + 4 + 2 + 5 + 8 - 3 - 3 = 18.5
EF= 1.4 – 0.03 * Σ (Pesoi *Valor asignadoi)
EF = 1.4 – 0.03 * 21
EF = 0.77

Los casos de uso ajustados resultan:
UCP= UUCP * TCF * EF
UCP= 95 * 1.045 * 0.77
UCP= 76.44175

3.2.7 Estimación del esfuerzo.

E = UCP * CF.

E: Esfuerzo estimado en horas hombres.

CF: Factor de conversión.

- Se contabilizan cuántos factores de los que afectan al factor de ambiente están por debajo del valor medio (3), para los factores E1 a E6.
- Se contabilizan cuántos factores de los que afectan al factor de ambiente están por encima del valor medio (3), para los factores E7 y E8.

- Si el total es 2 o menos, se utiliza el factor de conversión 20 horashombre/Punto de Casos de Uso, es decir, un Punto de Caso de Uso toma 20 horas-hombre.
- Si el total es 3 o 4, se utiliza el factor de conversión 28 horas-hombre/Punto de Casos de Uso, es decir, un Punto de Caso de Uso toma 28 horas hombre.
- Si el total es mayor o igual que 5, se recomienda efectuar cambios en el proyecto, ya que se considera que el riesgo de fracaso del mismo es demasiado alto.

En este proyecto si se analizan los valores tabulados anteriormente, es posible percatarse de que el total es 2, por lo que:

CF = 20 horas-hombre/punto de caso de uso.

El esfuerzo en horas hombres está dado por:

E = UCP * CF.

E =76.44175 * 20 horas/hombre.

E = 1.528.835 horas/hombre.

E ≈1.529 horas/hombre.

Duración:

Trabajando los 25 días del mes y 10 horas como promedio cada día se obtiene:
Duración en días = Total de horas /hombre entre 10 horas al día
Duración en días = 1.529 /10
Duración en días ≈153 días.
Duración en meses = Total de días /25 días por mes
Duración en meses = 153 /25
Duración en meses = 6.12

El proyecto se realizará aproximadamente en 6 meses.

Actividad	%Esfuerzo	Valor Esfuerzo
Análisis	10	152.9
Diseño	20	305.8
Implementación	40	611.6
Prueba	15	229.35
Sobrecarga	15	229.35
Total	100	1529

Tabla 14: Esfuerzo del Proyecto Desarrollado.

Cálculo de costo.

Tomando como salario promedio mensual $400.00 MN.

Costo CUP = 6.12 meses * $400.00.

Costo CUP = $2448

Costo CUC = $97.92.

Por tanto:

Se concluye que el proyecto tiene un costo asociado de $2448CUP (equivalente a $97.92CUC).

3.3 Beneficios tangibles e intangibles

La aplicación web fue desarrollada para convertirse en una solución general, capaz de aplicarse a cualquier empresa que precise una realización y control del plan de seguridad informática. Los beneficios obtenidos con el desarrollo del software permiten implementar una aplicación que realice el plan de seguridad informática de la Universidad de Cienfuegos y cumpla con todos los requerimientos propios de la entidad.

3.4 Análisis de costos y beneficios

Para analizar si es factible o no realizar el sistema informático, es necesario analizar el costo de realizar dicho sistema informático contra los beneficios de realizar el mismo.

El sistema informático naciente de la presente investigación, no implica costo alguno y no necesita una inversión en medios técnicos para la Universidad de Cienfuegos, sin embargo, a la elaboración de cualquier sistema informático va aparejado un costo y su justificación económica viene dado por los beneficios que este produce. Con el desarrollo de este sistema informático se logra agilizar el control y gestión de la información disminuyendo en gran manera el tiempo requerido para la elaboración del plan de seguridad informática en la Universidad de Cienfuegos.

La elaboración del sistema informático propuesto, representa un costo total de $2448MN y se puede llevar a cabo por una sola persona en un período de 6 meses.

Los beneficios obtenidos con el desarrollo del sistema informático permiten agilizar el control y gestión de la información disminuyendo en gran manera el tiempo requerido para la elaboración del plan de seguridad informática en la Universidad de Cienfuegos.

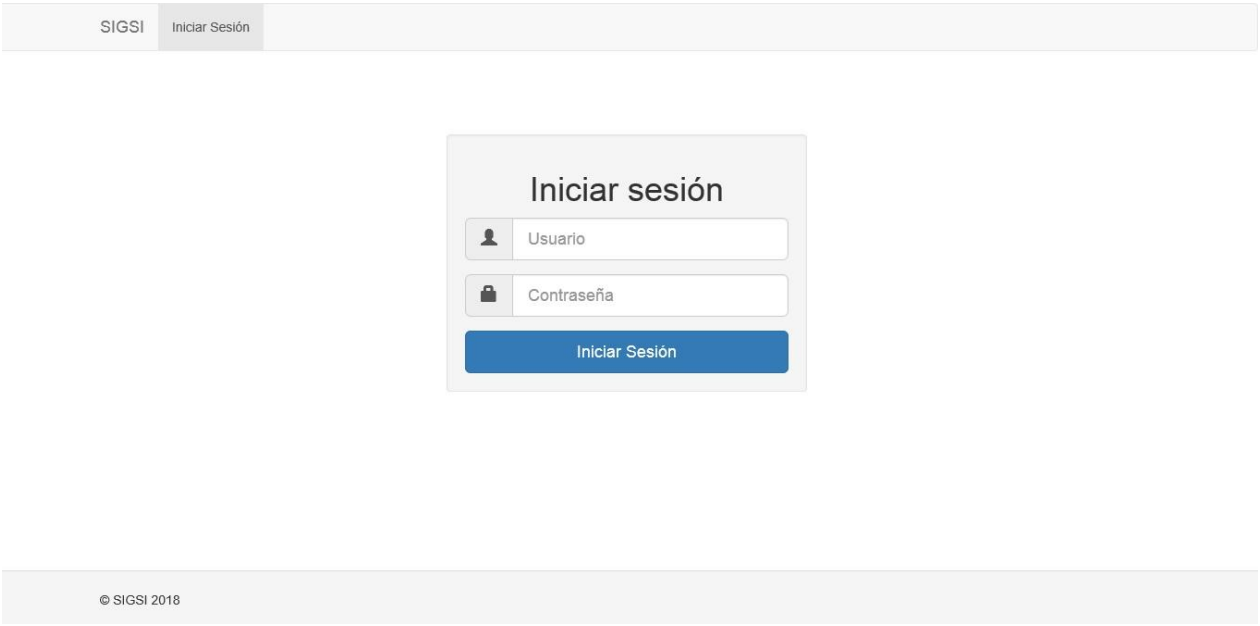
De esta manera se logra que los esfuerzos empleados en el desarrollo del sistema informático estén encaminados al cumplimiento de los objetivos planteados.

3.5 Diseño de Pruebas Funcionales

Un aspecto crucial en el control de calidad del desarrollo de software son las pruebas y, dentro de estas, las pruebas funcionales, en las cuales se hace una verificación dinámica del comportamiento de un sistema, basada en la observación de un conjunto seleccionado de ejecuciones controladas o casos de prueba.

Las pruebas funcionales son aquellas que se aplican al producto final, y permiten detectar en que puntos el producto no cumple sus especificaciones, es decir, comprobar su funcionalidad.

3.5.1 Caso de Pruebas Funcionales página de Autenticación:



Validaciones: La validación se hace en el evento “onClick” del Botón *Iniciar Sesión*, con las siguientes reglas:

- Usuario: No puede ser nulo y existe en la Base de Datos. (Obligatorio)

- Contraseña: No puede ser nulo y coincide con la contraseña del usuario en la Base de Datos. (Obligatorio)

Si la validación no tuvo éxito saldrá un mensaje especificando alguno de los siguientes errores:

Usuario:

- - Debe introducir un nombre de usuario.
  (Ubicado debajo del campo contraseña).
  Contraseña:
- - Debe introducir la contraseña.
  (Ubicado debajo del campo contraseña)

Si alguno de los dos campos está incorrecto entonces mostrará:

-Usuario o contraseña incorrectos

Resultados de la prueba funcional página de Autenticación:

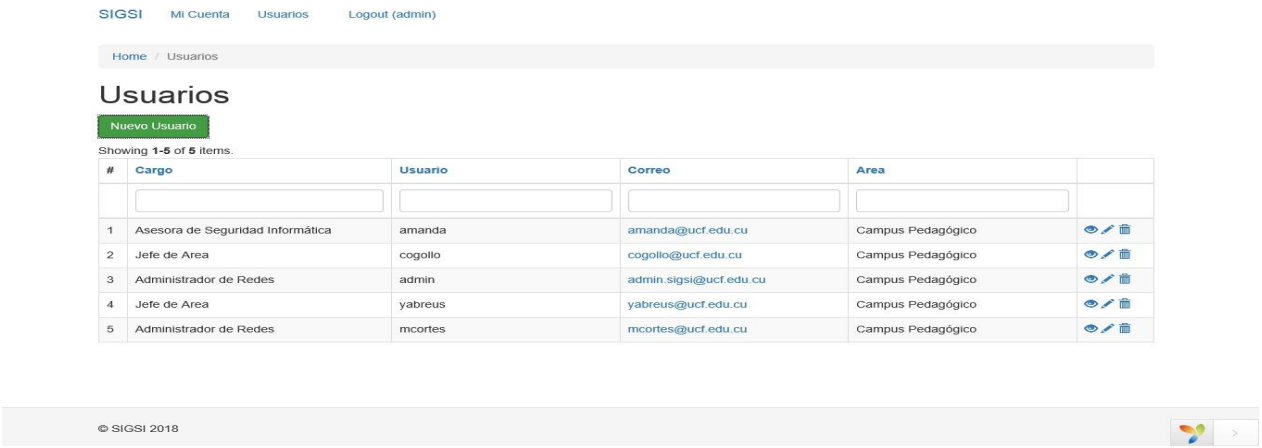
Esta prueba funcional arrojó los siguientes errores:

Al introducir un nombre de usuario o contraseña incorrectos el sistema no lanzaba la validación Usuario o contraseña incorrectos.

3.5.2 Caso de Pruebas Funcionales para Gestionar Usuarios.

Sección principal de Gestionar Usuarios (A).

Se divide en tres partes: Menú, Operaciones e Información y se distribuyen de la siguiente manera:



Menú: Tiene asociada una operación general para el usuario, esta es:

- Insertar Usuario.

Operaciones:

- Insertar Usuario.

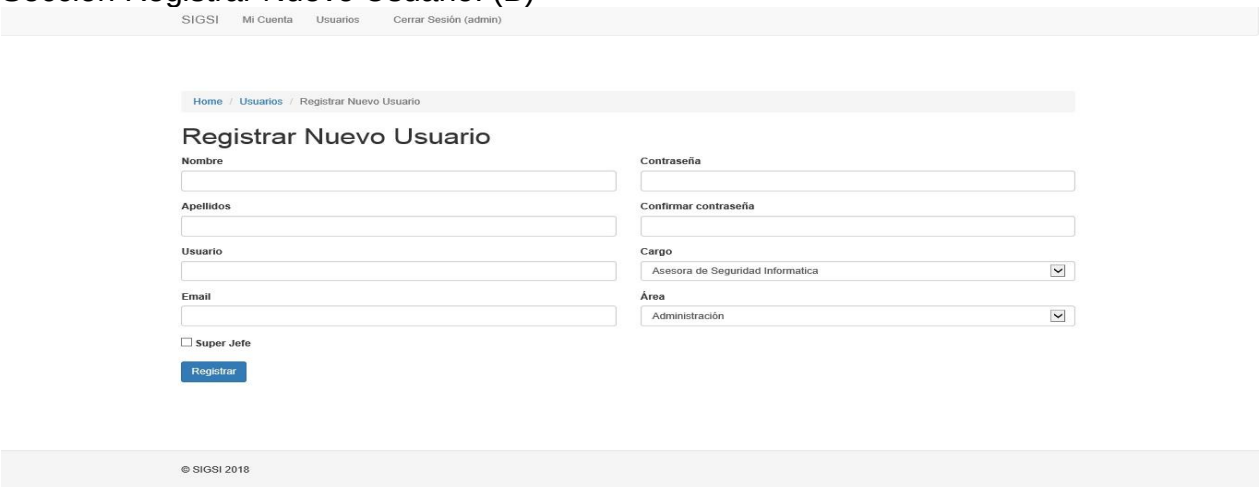
Información:

- Información general de todos los usuarios existentes en el sistema.

Validaciones:

- Si el usuario elimina algún usuario del sistema este mostrará una confirmación de eliminación, al ser aceptada, el sistema elimina el usuario.

Sección Registrar Nuevo Usuario: (B)



Invocada por: A

Destino: A

Validaciones: La validación se hace en el evento de “Onclick” del botón Registrar, con las siguientes reglas:

- Nombre: Nombre del usuario que se va a registrar en el sistema.
- Apellidos: Apellidos del usuario que se va a registrar en el sistema.
- Usuario: Nombre con que el usuario se registrará en el sistema. (Obligatorio).
- Email: Dirección de un correo electrónico del usuario. (Obligatorio)
- Contraseña: Cadena de caracteres, mínimo de 8 caracteres. (Obligatorio)
- Confirmar contraseña: Repetir la cadena de caracteres, mínimo de 8 caracteres. (Obligatorio)
- Cargo: Lista desplegable que muestra los cargos disponibles.
- Área: Lista desplegable que muestra la lista de áreas disponibles.

Si la validación no tuvo éxito saldrá un mensaje especificando alguno de los siguientes errores:

Nombre:

- - Campo requerido

  (Ubicado debajo del campo Nombre)

  Apellidos:

- - Campo requerido

  (Ubicado debajo del campo Apellidos)

Usuario:

- - Campo requerido
- - El usuario seleccionado ya existe

(Ubicado debajo del campo Usuario).

Email:

- - Campo requerido
- - El Email seleccionado ya existe.
- - Formato no válido.

(Ubicado debajo del campo Email)

Contraseña:

- - Campo requerido.
- - Mínimo 8 caracteres).

(Ubicado debajo del campo contraseña)

Confirmar contraseña:

- -Campo requerido
- - Las contraseñas no coinciden

(Ubicado debajo del campo Confirmar contraseña)

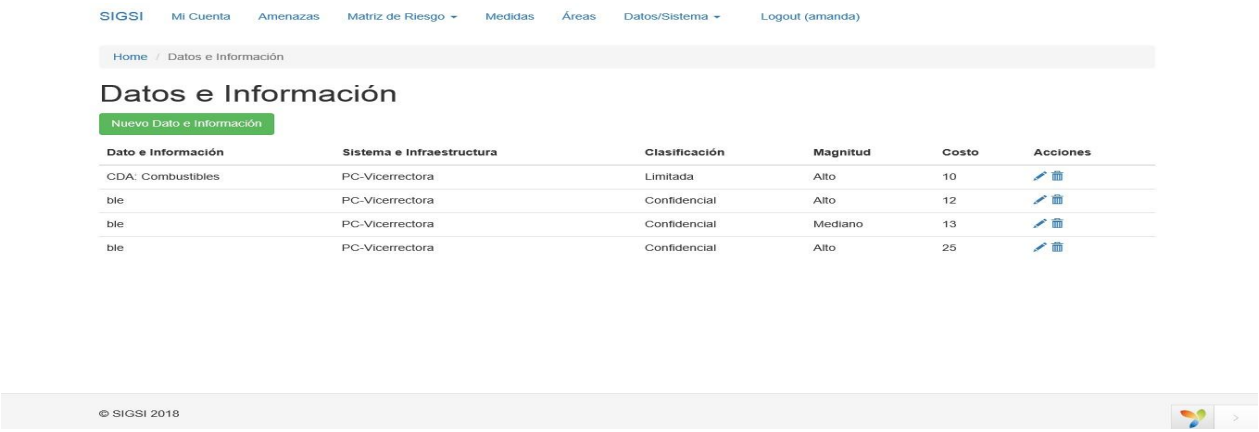
Resultados de la prueba funcional Gestionar Usuarios:
Esta prueba funcional arrojó los siguientes errores:

En el caso de que el campo Nombre o el campo Apellidos quedasen vacíos no mostraba la validación Campo requerido.
Cuando se introducía una contraseña aceptaba cualquiera así tuviese un solo dígito o letra.
El sistema podía introducir un nuevo usuario con todos sus campos vacíos.
No identificaba si el email introducido ya existía

3.5.3 Casos de Pruebas Funcionales para Gestionar Datos e Información.

Sección principal de Gestionar Datos e Información (A).

Se divide en tres partes: Menú, Operaciones e Información y se distribuyen de la siguiente manera:



Menú: Tiene asociada una operación general para el usuario, esta es:

- Insertar Dato e Información.

Operaciones:

- Insertar Dato e Información.

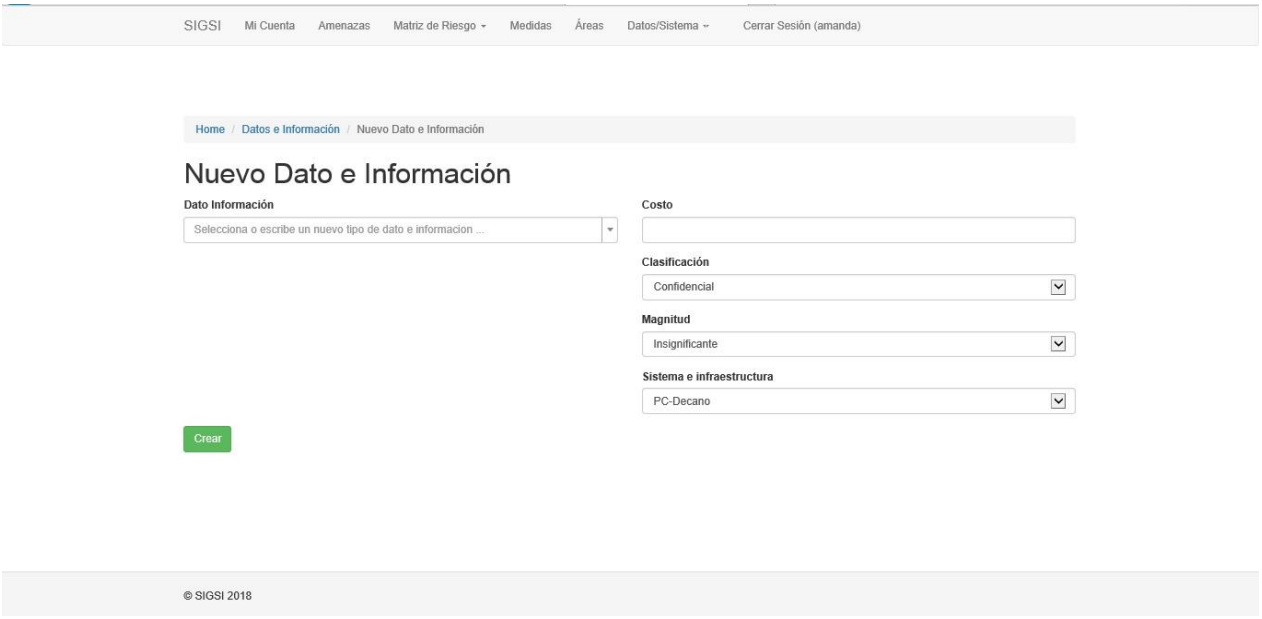
Información:

- Información general de todos los Datos e Información existentes en el sistema.

Validaciones:

- Si el usuario elimina algún dato e información del sistema este mostrará una confirmación de eliminación, al ser aceptada, el sistema elimina el dato e información.

Sección insertar nuevo Dato e Información: (B)



Invocada por: A

Destino: A

Validaciones: La validación se hace en el evento de “Onclick” del botón Crear, con las siguientes reglas:

- Dato Información: Nombre de la información
- Costo: Costo estimado de recuperación
- Clasificación: Lista desplegable que muestra las clasificaciones disponibles.
- Magnitud: Lista desplegable que muestra clasificaciones para la magnitud disponibles.
- Sistema e Infraestructura: Lista desplegable que muestra los sistemas e infraestructura disponibles.

Si la validación no tuvo éxito saldrá un mensaje especificando alguno de los siguientes errores:

Dato e información:

- - Campo requerido

(Ubicado debajo del campo dato e información)

Costo:

- - Campo requerido
- -El costo debe ser un número

(Ubicado debajo del campo Costo)

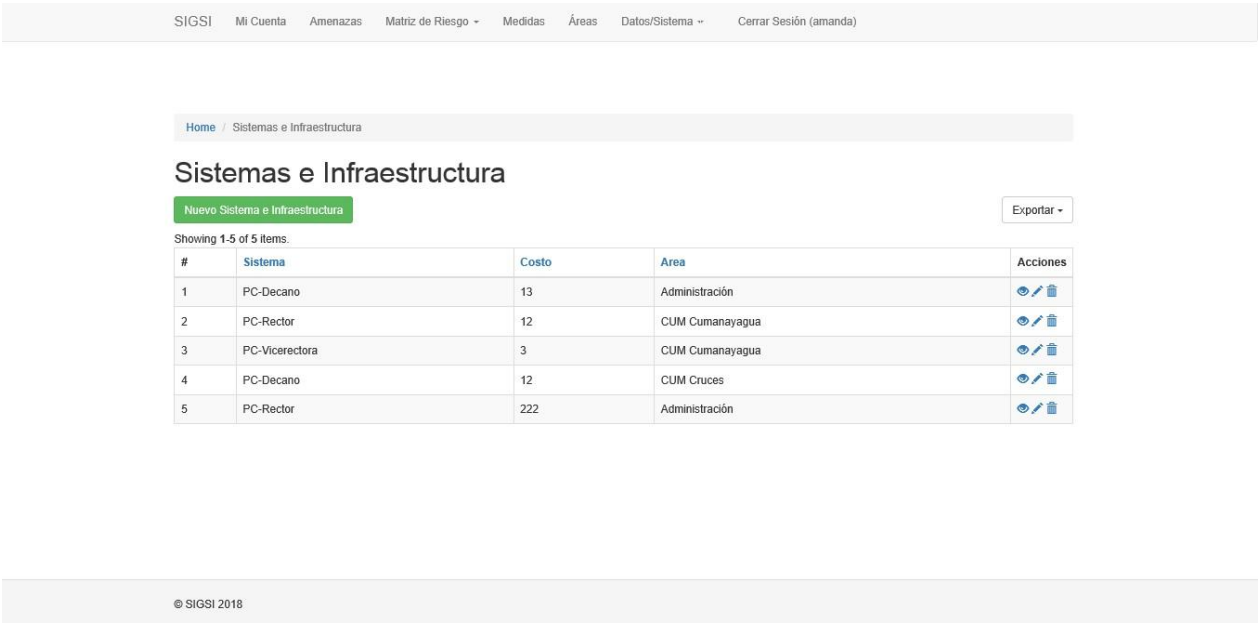
Resultados de la prueba funcional Gestionar Datos e Información:
Esta prueba funcional arrojó los siguientes errores:

Si no se introducía un nuevo dato e información el sistema no mostraba la validación campo requerido y además añadía ese campo vacío.
El costo podía ser una palabra.
Se podía crear el dato o información sin haberle agregado una infraestructura

3.5.4 Caso de Pruebas Funcionales del Caso de Uso Gestionar Infraestructura.

Sección principal de Gestionar Sistema e Infraestructura (A).

Se divide en tres partes: Menú, Operaciones e Información y se distribuyen de la siguiente manera:



Menú: Tiene asociada una operación general para el usuario, esta es:

- Insertar Sistema e Infraestructura.

Operaciones:

- Insertar Sistema e Infraestructura.

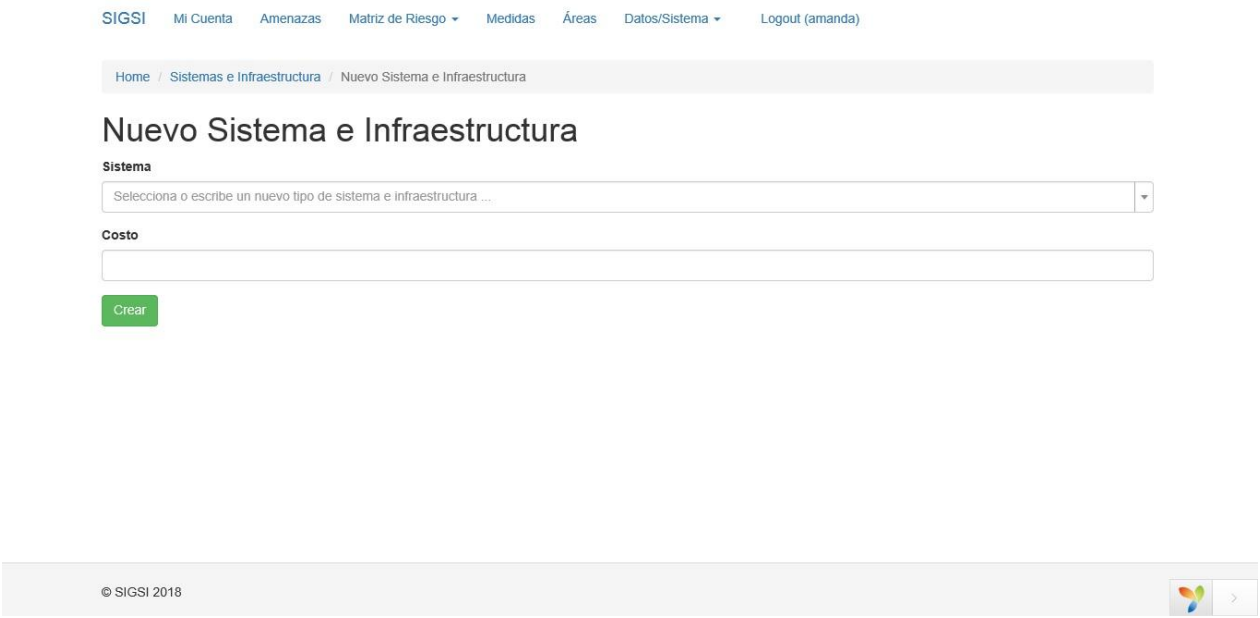
Información:

- Información general de todos los Sistemas e Infraestructura existentes en el sistema.

Validaciones:

- Si el usuario elimina algún Sistema e Infraestructura del sistema este mostrará una confirmación de eliminación, al ser aceptada, el sistema elimina el Sistema e Infraestructura.

Sección insertar nuevo Sistema e Infraestructura: (B)



Invocada por: A

Destino: A

Validaciones: La validación se hace en el evento de “Onclick” del botón Crear, con las siguientes reglas:

- Sistema: Nombre del sistema e infraestructura
- Costo: Costo estimado de recuperación

Si la validación no tuvo éxito saldrá un mensaje especificando alguno de los siguientes errores:

Sistema:

- - Campo requerido

(Ubicado debajo del campo Sistema)

Costo:

- - Campo requerido
- -El costo debe ser un número

(Ubicado debajo del campo Costo)

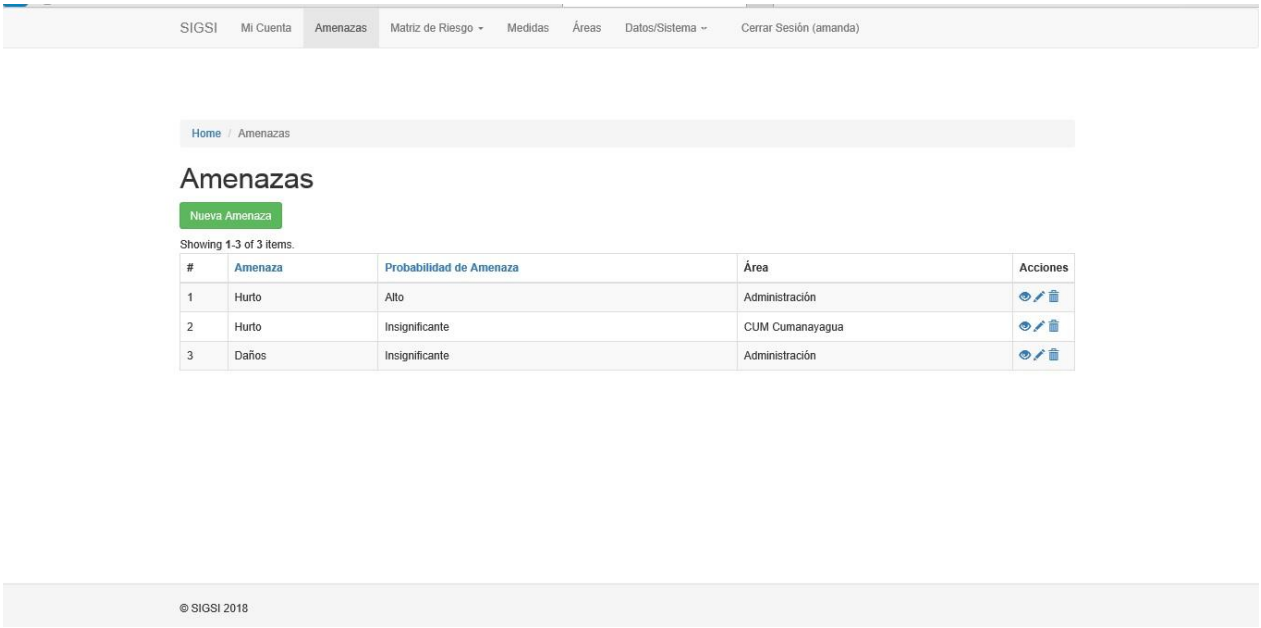
Resultados de la prueba funcional Gestionar Infraestructura:

Esta prueba funcional no arrojó errores:

3.5.5 Caso de Pruebas Funcionales para el Caso de Uso Gestionar Amenazas.

Sección principal de Gestionar Amenazas (A).

Se divide en tres partes: Menú, Operaciones e Información y se distribuyen de la siguiente manera:



Menú: Tiene asociada una operación general para el usuario, esta es:

- Insertar Amenazas.

Operaciones:

- Insertar Amenazas.

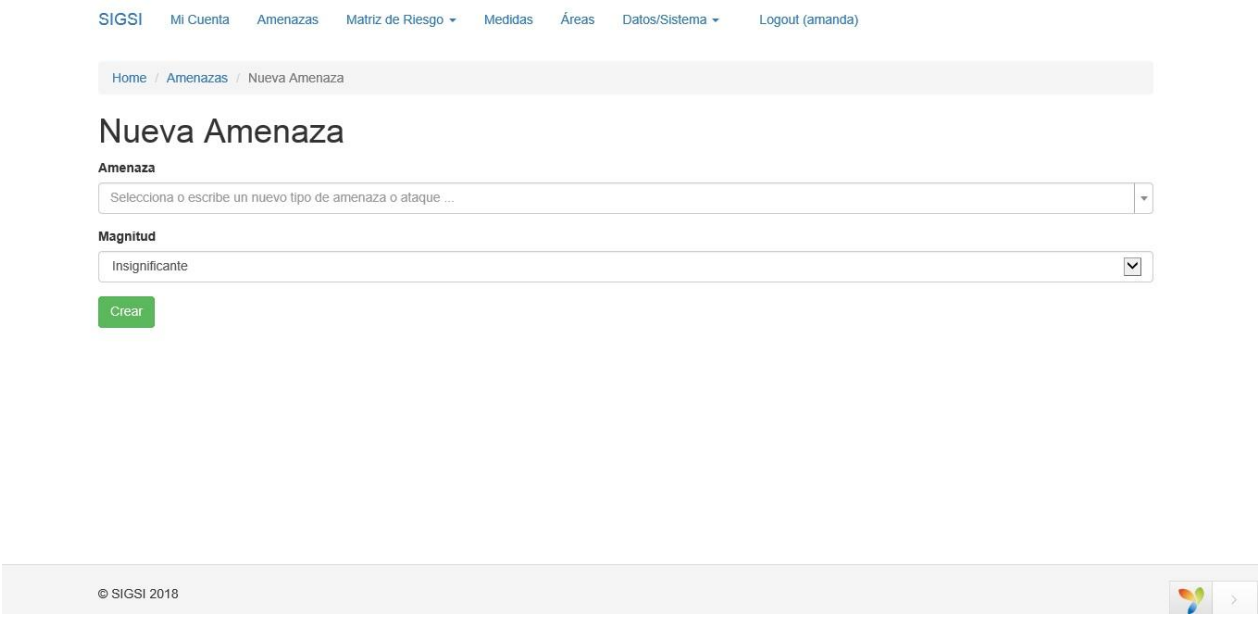
Información:

- Información general de todas las Amenazas existentes en el sistema.

Validaciones:

- Si el usuario elimina alguna amenaza del sistema este mostrará una confirmación de eliminación, al ser aceptada, el sistema elimina la amenaza.

Sección insertar nueva amenaza: (B)



Invocada por: A

Destino: A

Validaciones: La validación se hace en el evento de “Onclick” del botón Crear, con las siguientes reglas:

- Amenaza: Nombre de la amenaza
- Magnitud: Lista desplegable que muestra clasificaciones para la magnitud disponibles.

Si la validación no tuvo éxito saldrá un mensaje especificando alguno de los siguientes errores:

Amenaza:

- - Campo requerido
  (Ubicado debajo del campo Amenaza)

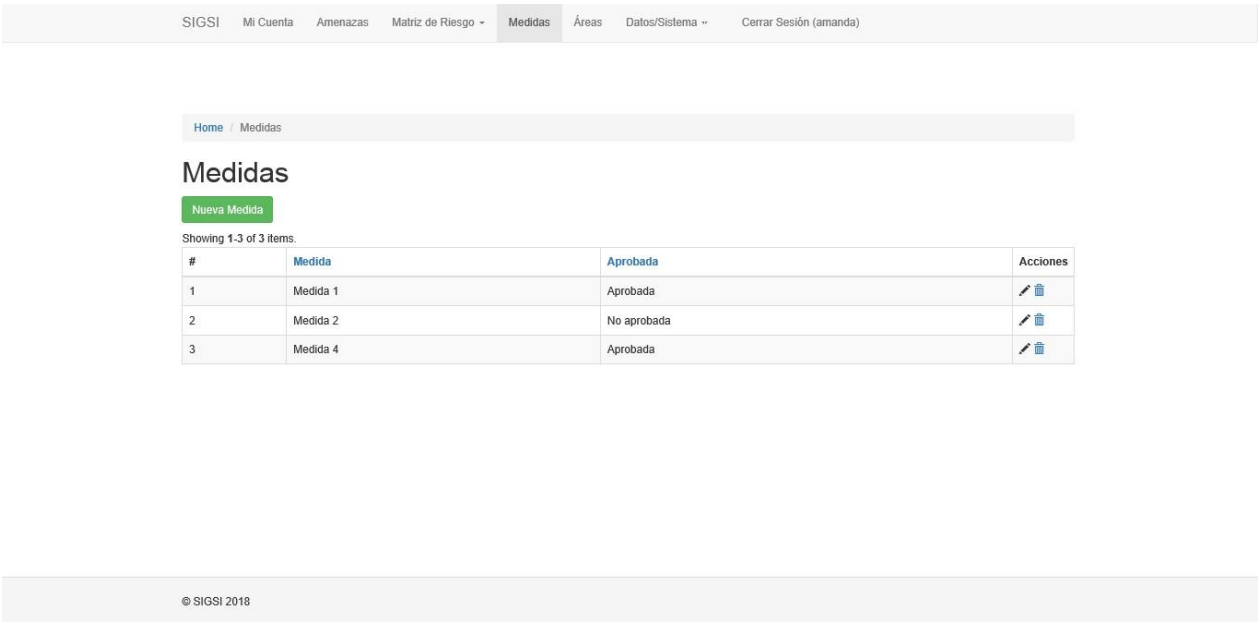
Resultados de la prueba funcional Gestionar Amenazas:

Esta prueba funcional arrojó los siguientes errores:
En caso de que el campo Amenaza se dejase vacío no lanzaba la validación campo requerido.

3.5.6 Caso de Pruebas Funcionales para el Caso de Uso Gestionar Medidas.

Sección principal de Gestionar Medidas (A).

Se divide en tres partes: Menú, Operaciones e Información y se distribuyen de la siguiente manera:



Menú: Tiene asociada una operación general para el usuario, esta es:

- Insertar Medidas.

Operaciones:

- Insertar Medidas.

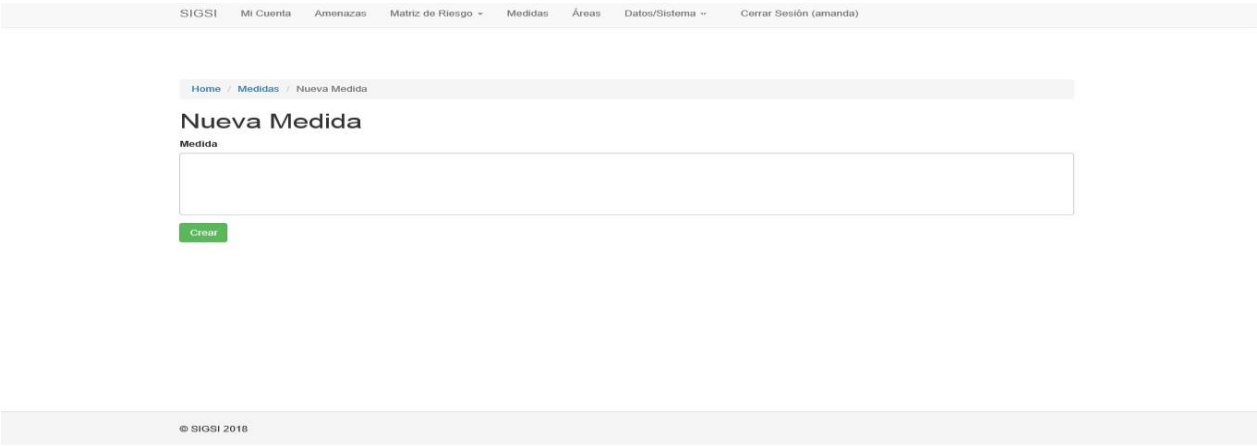
Información:

- Información general de todas las medidas existentes en el sistema.

Validaciones:

- Si el usuario elimina alguna medida del sistema este mostrará una confirmación de eliminación, al ser aceptada, el sistema elimina la medida.

Sección insertar nueva medida: (B)



Invocada por: A

Destino: A

Validaciones: La validación se hace en el evento de “Onclick” del botón Crear, con las siguientes reglas:

- Medida: Texto con la medida que se añadirá a ese punto

Si la validación no tuvo éxito saldrá un mensaje especificando alguno de los siguientes errores:

Medida:

- - Campo requerido
  (Ubicado debajo del campo Medida)

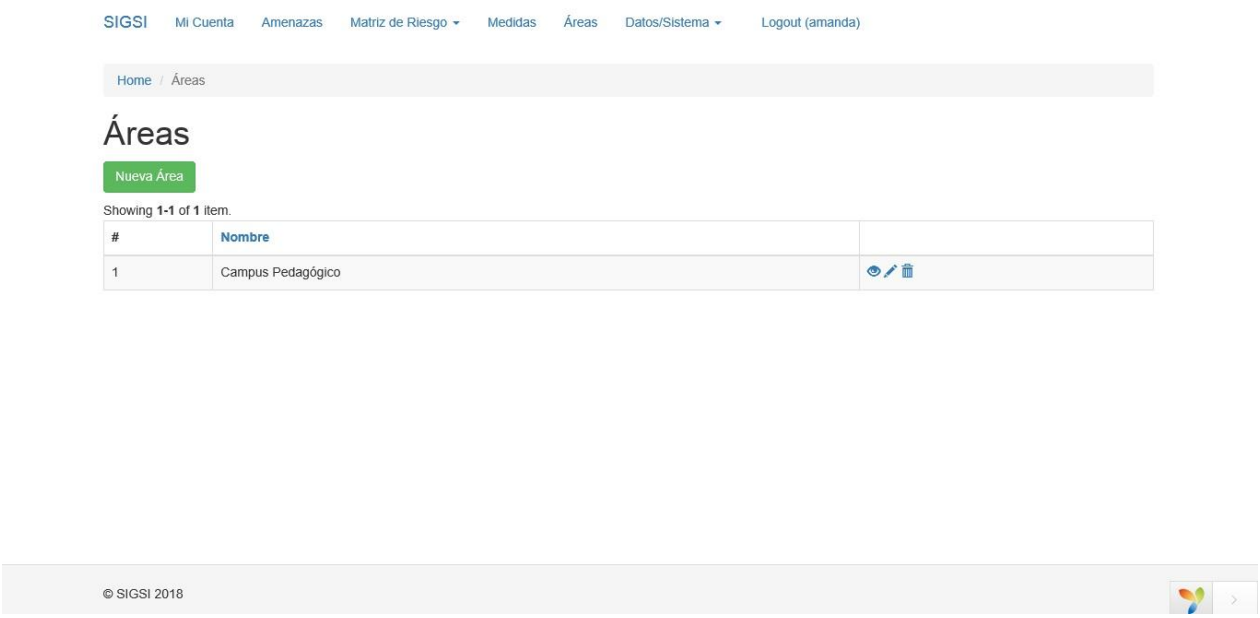
Resultados de la prueba funcional Gestionar Medidas:

Esta prueba funcional no arrojó errores:

3.5.7 Caso de Pruebas Funcionales para el Caso de Uso Gestionar Áreas.

Sección principal de Gestionar Áreas (A).

Se divide en tres partes: Menú, Operaciones e Información y se distribuyen de la siguiente manera:



Menú: Tiene asociada una operación general para el usuario, esta es:

- Insertar Áreas.

Operaciones:

- Insertar Áreas.

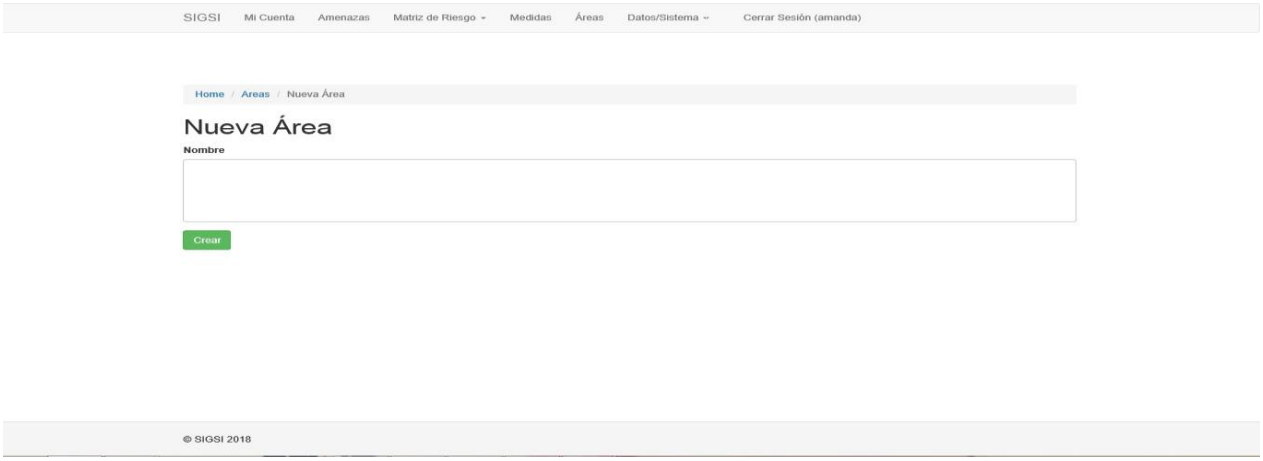
Información:

- Información general de todas las áreas existentes en el sistema.

Validaciones:

- Si el usuario elimina algún área del sistema este mostrará una confirmación de eliminación, al ser aceptada, el sistema elimina las áreas.

Sección insertar nueva área: (B)



Invocada por: A

Destino: A

Validaciones: La validación se hace en el evento de “Onclick” del botón Crear, con las siguientes reglas:

- Nombre: Texto con el nombre del área.

Si la validación no tuvo éxito saldrá un mensaje especificando alguno de los siguientes errores:

Nombre:

- - Campo requerido

(Ubicado debajo del campo Nombre)

Resultados de la prueba funcional Gestionar Áreas:

Esta prueba funcional no arrojó errores:

3.6 Conclusiones

En este capítulo se realizó el cálculo de factibilidad económica, concluyendo que el sistema propuesto trae consigo grandes beneficios en la confección y control del plan de seguridad informática de la Universidad de Cienfuegos, por lo que es factible la implementación de la herramienta propuesta, estimándose un tiempo de 6 meses para su construcción y su costo asciende a $2448aproximadamente.

Se diseñaron los casos de prueba funcionales permitiendo obtener una verificación dinámica del comportamiento del sistema, garantizando de esta forma el control de la calidad en el desarrollo del software. En la realización de estas pruebas funcionales se detectaron 10 errores en las entradas da datos y dándole solución a los mismos se logró validar el sistema ante este tipo de errores, garantizando así una mayor confiabilidad de la información.

Conclusiones

Los resultados del siguiente trabajo responden satisfactoriamente a los objetivos propuestos, por lo que se concluye:

- Se realizó para la confección del sistema propuesto un análisis del modo en que se gestiona de la seguridad informática, lo cual permitió lograr un mejor entendimiento del proceso e identificar las actividades objeto de automatización.

- Se desarrolló un sistema informático que gestiona correctamente el plan de seguridad Informática en la Universidad de Cienfuegos.

- El diseño de los casos de prueba funcional permitió obtener una verificación dinámica del comportamiento del sistema, garantizando de esta forma el control de la calidad en el desarrollo del software.

Recomendaciones

A pesar de que la investigación realizada cumplió con los objetivos trazados, se recomienda:

- Utilizar el sistema informático implementado para la gestión del plan de seguridad informática en otras universidades del país.

- Poner a prueba el sistema durante un periodo de tiempo significativo para poder comprobar de forma práctica sus funcionalidades y obtener los datos necesarios para su perfeccionamiento.

- Incorporar módulos que permitan el control y la auditoría informática.

.

Referencias bibliográficas

[1] A. Antúnez and N. Oduardo, Auditoria y Seguridad informática. Realidades y perspectivas en Cuba.[Documento en línea]. .

[2] J. Cano, “Concepto Extendido de la Mente Segura: Pensamiento Sistémico en Seguridad Informática.” [Online]. Available: http://www.criptored.upm.es/guiateoria/gt_m142x.htm. [Accessed: 12-Jun-2018].

[3] T. P. S. documentation and c. logical, “Information technology–Security techniques–Information security management systems–Requirements,” 2005.

[4] R. Montesino Perurena, W. Baluja García, and J. Porvén Rubier, “Gestión automatizada e integrada de controles de seguridad informática,” Ingeniería Electrónica, Automática y Comunicaciones, vol. 34, no. 1, pp. 40–58, 2013.

[5] M. E. Corti, G. Betarte, and R. De la Fuente, “Hacia una implementación Exitosa de un SGSI,” in IV Congreso Internacional de Auditoría y Seguridad de la Información, 2005.

[6] F. N. S. Solarte, E. R. E. Rosero, and M. del Carmen Benavides, “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001,” Revista Tecnológica-ESPOL, vol. 28, no. 5, 2015.

[7] “Inseguridad informática: un concepto dual en seguridad informática. | J. Cano | Revista de Ingeniería.” [Online]. Available: https://ojsrevistaing.uniandes.edu.co/ojs/index.php/revista/article/view/437. [Accessed: 12-Jun-2018].

[8] A. C. Nieves, “Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001: 2013,” 2017.

[9] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing octave allegro: Improving the information security risk assessment process,” Carnegie-mellon univ pittsburgh pa software engineering inst, 2007.

[10] A. Christopher and D. Autrey, Managing Information security risks. The OCTAVE Approach. SL: Addison-Wesley, 2003.

[11] A. Christopher and D. Autrey, “OCTAVE Criteria Versión 2.0,” Pittsburgh: Carniege Mellon–Software Engineering Institute, 2001.

[12] M. Bača and F. O. I. Varaždin, “The risk assessment of information system security,” Fakultet organizacije i informatike, Sveučilište u Zagrebu.< dostupno na http://cuc. carnet. hr/cuc2004/program/radovi/a5_baca/a5_full. pdf>,[očitano 07.10. 2010], 2004.

[13] M. Miranda Cairo, O. Valdés Puga, I. Pérez Mallea, R. Portelles Cobas, and R. Sánchez Zequeira, “Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática,” Revista Cubana de Ciencias Informáticas, vol. 10, no. 2, pp. 14–26, 2016.

[14] Y. Díaz-Ricardo, Y. Pérez-del Cerro, and D. Proenza-Pupo, “Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín,” Ciencias Holguín, vol. 20, no. 2, pp. 13–26, 2014.

[15] F. A. Amo, L. M. Normand, and F. J. S. Pérez, Introducción a la ingeniería del software. Delta Publicaciones, 2005.

[16] I. Sommerville, Ingeniería del software. Pearson Educación, 2005.

[17] I. Jacobson, G. Booch, and J. Rumbaugh, El proceso unificado de desarrollo de software/The unified software development process. Pearson Educación,, 2000.
[18] O. A. Pérez, “Cuatro enfoques metodológicos para el desarrollo de Software RUP–MSF–XP-SCRUM,” INVENTUM, vol. 6, no. 10, pp. 64–78, 2011.
[19] E. Hernández Orallo, El Lenguaje Unificado de Modelado (UML). .
[20] E. Hernández Orallo, “El lenguaje unificado de modelado (UML),” Recuperado el, vol. 20, 2000.
[21] “Rafael Menéndez-Barzanallana Asensio. Historia del desarrollo de aplicaciones Web. Universidad de Murcia.” [Online]. Available: http://www.um.es/docencia/barzana/DIVULGACION/INFORMATICA/Historia-desarrollo-aplicaciones-web.html. [Accessed: 12-Jun-2018].
[22] R. Barzanallana, “Historia del desarrollo de aplicaciones Web,” Universidad de Murcia. Recuperado el, vol. 29, 2012.
[23] J. J. Gutiérrez, “¿ Qué es un framework web,” Available in: http://www. lsi. us. es/~ javierj/investigacion_ficheros/Framework. pdf Accessed May, vol. 12, 2014.
[24] A. B. MySQL, MySQL. 2001.
[25] Á. Cobo, PHP y MySQL: Tecnología para el desarrollo de aplicaciones web. Ediciones Díaz de Santos, 2005.
[26] V. D. Varas, A. L. Agüero, A. E. Guzmán, and M. Martínez, “Importancia y beneficios de la accesibilidad web para todos,” in X Congreso sobre Tecnología en Educación & Educación en Tecnología (TE & ET)(Corrientes, 2015), 2015.
[27] J. J. Gutiérrez, M. J. Escalona, M. Mejías, and A. M. R. Quintero, “Modelos de Pruebas para Pruebas del Sistemas.,” in DSDM, 2006.
[28] “UML - Analisis del negocio.” [Online]. Available: https://www.scribd.com/doc/2568110/UML-Analisis-del-negocio. [Accessed: 12-Jun-2018].
[29] J. Rumbaugh, I. Jacobson, and G. Booch, “El proceso unificado de desarrollo de software,” Addison-Wesley. Madrid, España, 2000.
[30] “IBM Knowledge Center - Modelos lógicos de datos.” [Online]. Available: https://www.ibm.com/support/knowledgecenter/es/SS9UM9_9.1.2/com.ibm.datatools.logical.ui.doc/topics/clogmod.html. [Accessed: 12-Jun-2018].
[31] “IBM Knowledge Center - Modelos físicos de datos.” [Online]. Available: https://www.ibm.com/support/knowledgecenter/es/SS9UM9_9.1.0/com.ibm.datatools.core.ui.doc/topics/cphysmod.html. [Accessed: 12-Jun-2018].
[32] Y. D. González and Y. F. Romero, “Patrón Modelo-Vista-Controlador.,” Revista Telem@ tica, vol. 11, no. 1, pp. 47–57, 2012.

.

Bibliografía

[1] J. J. Gutiérrez, "¿ Qué es un framework web," *Available in: http://www. lsi. us. es/~ javierj/investigacion_ficheros/Framework. pdf Accessed May*, vol. 12, 2014.

[2] M. P. Baptiste, N. Castaño, D. Cárdenas López, F. de P. Gutiérrez, D. Gil, and C. A. Lasso, "Análisis de riesgo y propuesta de categorización de especies introducidas para Colombia," 2010.

[3] E. E. Luna, L. Espinoza, and L. García, A*nálisis de riesgos*. Boaco–Nicaragua: Agencia Suiza para el Desarrollo y la Cooperación (COSUDE), 2001.

[4] J. H. Barón, J. E. N. Mac Leod, and S. S. Rivera, "Análisis de Riesgos."

[5] Y. León Perdomo, A. Enrique Góngora Rodríguez, and A. Febles Estrada, "Aplicando métricas de calidad a proyectos y procesos durante las pruebas exploratorias," *Revista Cubana de Ciencias Informáticas*, vol. 7, no. 2, pp. 193–205, 2013.

[6] A. Antúnez and N. Oduardo, "Auditoria y Seguridad informática. Realidades y perspectivas en Cuba." .

[7] A. Antúnez and N. Oduardo, *Auditoria y Seguridad informática. Realidades y perspectivas en Cuba.[Documento en línea]*. .

[8] J. Cano, "Concepto Extendido de la Mente Segura: Pensamiento Sistémico en Seguridad Informática." [Online]. Available: http://www.criptored.upm.es/guiateoria/gt_m142x.htm. [Accessed: 12-Jun-2018].

[9] R. D. Martínez Vidal, Y. H. Montero Mauro, and M. E. Pedrosa Borrini, "Creencias epistemológicas, estrategias de búsqueda de información, y criterios para validar la información de la Web," *Revista electrónica de investigación educativa*, vol. 12, pp. 1–26, 2010.

[10] O. A. Pérez, "Cuatro enfoques metodológicos para el desarrollo de Software RUP–MSF–XP-SCRUM," *INVENTUM*, vol. 6, no. 10, pp. 64–78, 2011.

[11] G. M. Villalobos, G. D. C. Sánchez, and D. A. B. Gutiérrez, "Diseño de framework web para el desarrollo dinámico de aplicaciones," *Scientia et technica*, vol. 1, no. 44, pp. 178–183, 2010.

[12] A. C. Nieves, "Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001: 2013," 2017.

[13] A. H. Velasco Melo, "EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27 001," *Revista de Derecho*, pp. 333–366, 2008.

[14] E. Hernández Orallo, "El lenguaje unificado de modelado (UML)," *Recuperado el*, vol. 20, 2000.

[15] J. Rumbaugh, I. Jacobson, and G. Booch, "El proceso unificado de desarrollo de software," *Addison-Wesley. Madrid, España*, 2000.

[16] I. Jacobson, G. Booch, and J. Rumbaugh, *El proceso unificado de desarrollo de software/The unified software development process*. Pearson Educación,, 2000.

[17] D. Gómez-Selemeneva, B. Blanco-Camping, and J. R. Conde-Camilo, "El Sistema de Control Interno para el Perfeccionamiento de la Gestión Empresarial en Cuba (Internal Control System for the Improvement of Corporate Governance in Cuba)," 2013.

[18] "Enrique Buono's blog - Red Colaborativa Postgrado UCV." [Online]. Available: http://kuainasi.ciens.ucv.ve/red_educativa/blogs/user/enriquebuono. [Accessed: 12-Jun-2018].

[19] R. L. H. Claro and D. G. Navarro, "Estándares de diseño Web," *Ciencias de la Información*, vol. 41, no. 2, pp. 69–71, 2010.
[20] C. Gil and R. Alberto, "Estructura básica del proceso unificado de desarrollo de software," 2006.
[21] F. L. Bryan and W. H. Organization, "Evaluaciones por análisis de peligros en puntos críticos de control: guía para identificar peligros y evaluar riesgos relacionados con la preparación y la conservación de alimentos," 1992.
[22] R. Montesino Perurena, W. Baluja García, and J. Porvén Rubier, "Gestión automatizada e integrada de controles de seguridad informática," *Ingeniería Electrónica, Automática y Comunicaciones*, vol. 34, no. 1, pp. 40–58, 2013.
[23] "Gestión automatizada e integrada de controles de seguridad informática." [Online]. Available: http://scielo.sld.cu/scielo.php?pid=S1815-59282013000100004&script=sci_arttext&tlng=pt. [Accessed: 12-Jun-2018].
[24] A. Ramírez Castro and Z. Ortiz Bayona, "Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios," *Ingeniería*, vol. 16, no. 2, 2011.
[25] Á. M. V. Aponte, "Guía comparativa de Frameworks para los lenguajes HTML 5, CSS y JavaScript para el desarrollo de aplicaciones Web," Universidad Tecnológica de Pereira. Facultad de Ingenierías Eléctrica, Electrónica, Física y Ciencias de la Computación. Ingeniería de Sistemas y Computación, 2014.
[26] Center for History and New Media, "Guía rápida." [Online]. Available: http://zotero.org/support/quick_start_guide.
[27] M. E. Corti, G. Betarte, and R. De la Fuente, "Hacia una implementación Exitosa de un SGSI," in *IV Congreso Internacional de Auditoría y Seguridad de la Información*, 2005.
[28] G. Mendoza González, *Herramienta de Desarrollo Netbeans*. Colombia, 2008.
[29] R. Barzanallana, "Historia del desarrollo de aplicaciones Web," *Universidad de Murcia. Recuperado el*, vol. 29, 2012.
[30] "IBM Knowledge Center - Modelos lógicos de datos." [Online]. Available: https://www.ibm.com/support/knowledgecenter/es/SS9UM9_9.1.2/com.ibm.datatools.logical.ui.doc/topics/clogmod.html. [Accessed: 12-Jun-2018].
[31] V. D. Varas, A. L. Agüero, A. E. Guzmán, and M. Martínez, "Importancia y beneficios de la accesibilidad web para todos," in *X Congreso sobre Tecnología en Educación & Educación en Tecnología (TE & ET)(Corrientes, 2015)*, 2015.
[32] T. P. S. DOCUMENTATION and C. LOGICAL, "Information technology–Security techniques–Information security management systems–Requirements," 2005.
[33] I. Sommerville, *Ingeniería del software*. Pearson Educación, 2005.
[34] J. J. Cano, "Inseguridad informática: un concepto dual en seguridad informática.," *Revista de Ingeniería*, no. 19, pp. 40–44, 2004.
[35] "Inseguridad informática: un concepto dual en seguridad informática. | J. Cano | Revista de Ingeniería." [Online]. Available: https://ojsrevistaing.uniandes.edu.co/ojs/index.php/revista/article/view/437. [Accessed: 12-Jun-2018].
[36] X. Ferré and A. M. Moreno, "Integración de la IPO en el Proceso de Desarrollo de la Ingeniería del Software: Propuestas Existentes y Temas a Resolver," *Actas de Interacción*, 2004.
[37] F. A. Amo, L. M. Normand, and F. J. S. Pérez, *Introducción a la ingeniería del software*. Delta Publicaciones, 2005.

[38] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process," CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2007.
[39] "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process." [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419. [Accessed: 12-Jun-2018].
[40] J. C. Moreno and M. M. Marciszack, "La Usabilidad Desde La Perspectiva De La Validación de Requerimientos No Funcionales Para Aplicaciones Web," *Córdoba: Universidad Tecnológica Nacional*, 2013.
[41] A. Orjuela Duarte and M. Rojas, "Las metodologías de desarrollo ágil como una oportunidad para la ingeniería del software educativo," *Revista Avances en Sistemas e Informática*, vol. 5, no. 2, 2008.
[42] "Los patrones de diseño son el Origen de los Frameworks ? - posted by Enrique Buono at Red Colaborativa Postgrado UCV." [Online]. Available: http://kuainasi.ciens.ucv.ve/red_educativa/blogs/43?language_id=1. [Accessed: 12-Jun-2018].
[43] A. Christopher and D. Autrey, *Managing Information security risks*. The OCTAVE Approach. SL: Addison-Wesley, 2003.
[44] C. J. Alberts and A. Dorofee, *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., 2002.
[45] R. Gómez, D. H. Pérez, Y. Donoso, and A. Herrera, "Methodology and Governance of the IT Risk Management," *Revista de Ingeniería*, no. 31, pp. 109–118, 2010.
[46] "Methodology and Governance of the IT Risk Management." [Online]. Available: http://www.scielo.org.co/scielo.php?pid=S0121-49932010000100012&script=sci_arttext&tlng=pt. [Accessed: 12-Jun-2018].
[47] F. N. S. Solarte, E. R. E. Rosero, and M. del Carmen Benavides, "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001," *Revista Tecnológica-ESPOL*, vol. 28, no. 5, 2015.
[48] "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001 | Solarte Solarte | Revista Tecnológica - ESPOL." [Online]. Available: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456. [Accessed: 12-Jun-2018].
[49] M. Miranda Cairo, O. Valdés Puga, I. Pérez Mallea, R. Portelles Cobas, and R. Sánchez Zequeira, "Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática," *Revista Cubana de Ciencias Informáticas*, vol. 10, no. 2, pp. 14–26, 2016.
[50] F. Chiesa, "Metodología para selección de sistemas ERP," *Reportes técnicos en ingeniería del software*, vol. 6, no. 1, pp. 17–37, 2004.
[51] J. J. Gutiérrez, M. J. Escalona, M. Mejías, and A. M. R. Quintero, "Modelos de Pruebas para Pruebas del Sistemas.," in *DSDM*, 2006.
[52] J. A. H. Pérez, Y. O. Leyva, S. R. Betancourt, and I. L. Rodríguez, "Módulo de gestión de incidencias y acciones de la plataforma de gestión de recursos de inventarios de hardware y sofware," *Cuba: XI Seminario Iberoamericano de Seguridad en las Tecnologías de la Información*, 2013.
[53] A. B. MySQL, *MySQL*. 2001.
[54] A. Christopher and D. Autrey, "OCTAVE Criteria Versión 2.0," *Pittsburgh: Carniege*

Mellon–Software Engineering Institute, 2001.
[55] M. Sosonkin, "OCTAVE: operationally critical threat, asset and vulnerability evaluation," *Polytechnic University, Apr*, 2005.
[56] Y. D. González and Y. F. Romero, "Patrón Modelo-Vista-Controlador.," *Revista Telem@ tica*, vol. 11, no. 1, pp. 47–57, 2012.
[57] Á. Cobo, *PHP y MySQL: Tecnología para el desarrollo de aplicaciones web*. Ediciones Díaz de Santos, 2005.
[58] Y. G. Duque *et al.*, "Plan de seguridad informática."
[59] P. Cáceres, E. Marcos, and G. Kybele, "Procesos ágiles para el desarrollo de aplicaciones Web," *Taller de Web Engineering de las Jornadas de Ingeniería del Software y Bases de Datos de*, vol. 2001, 2001.
[60] "Rafael Menéndez-Barzanallana Asensio. Historia del desarrollo de aplicaciones Web. Universidad de Murcia." [Online]. Available: http://www.um.es/docencia/barzana/DIVULGACION/INFORMATICA/Historia-desarrollo-aplicaciones-web.html. [Accessed: 12-Jun-2018].
[61] Y. Díaz-Ricardo, Y. Pérez-del Cerro, and D. Proenza-Pupo, "Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín," *Ciencias Holguín*, vol. 20, no. 2, pp. 13–26, 2014.
[62] Y. Díaz, Y. Pérez, and D. Proenza, "Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín/System for the Management of the Information of Informatics Security at the Medical Sciences University of Holguín," *Holguín Ciencias*, pp. 1–14, 2014.
[63] R. Montero-Martínez, "Sistemas de gestión de seguridad y salud ocupacional y procesos basados en el comportamiento: aspectos claves para una implementación y gestión exitosas," *Ingeniería Industrial*, vol. 32, no. 1, 2011.
[64] R. Sanchis, R. Poler, and Á. Ortiz, "Técnicas para el Modelado de Procesos de Negocio en Cadenas de Suministro," *Información tecnológica*, vol. 20, pp. 29–40, 2009.
[65] M. Bača and F. O. I. Varaždin, "The risk assessment of information system security," *Fakultet organizacije i informatike, Sveučilište u Zagrebu.< dostupno na http://cuc. carnet. hr/cuc2004/program/radovi/a5_baca/a5_full. pdf>,[očitano 07.10. 2010]*, 2004.
[66] "UML - Analisis del negocio." [Online]. Available: https://www.scribd.com/doc/2568110/UML-Analisis-del-negocio. [Accessed: 12-Jun-2018].

Anexos

Documentos, imágenes, tablas, gráficos que complementan el contenido o conocimiento del trabajo de diploma, pero que por tamaño en hojas del cuerpo del documento no es posible incluirlo.

Todos los anexos deben ser referenciados en el cuerpo del documento.

Anexo A- Fichas.

Anexo A1-Ficha de Amenazas

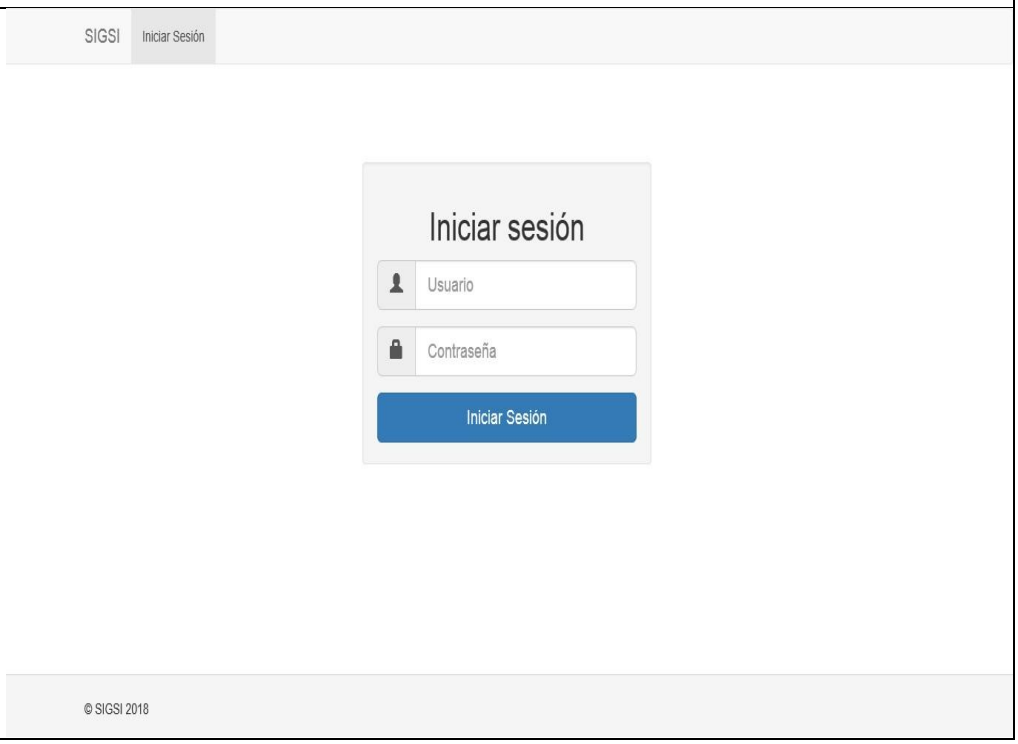
Tipo de Amenaza o Ataque	**Probabilidad de Amenaza**			
Actos originados por la criminalidad común y motivación política	**Insignificante (Ninguna)**	**Baja**	**Mediana**	**Alta**
Allanamiento (ilegal, legal)				
Persecución (civil, fiscal, penal)				
Orden de secuestro / Detención				
Sabotaje (ataque físico y electrónico)				
Daños por vandalismo				
Extorsión				

Anexo A2-Ficha de Datos e Información

Elementos de Información	**Clasificación**				**Magnitud de Daño**			
Datos e Información	**Confidencial**	**Limitada**	**Ordinaria**	**Costo estimado de recuperación (tiempo, económico, material, imagen, emocional)**	**Insignificante (Ninguno)**	**Bajo**	**Mediano**	**Alto**

Anexo B- Descripción de los casos de uso del sistema

Anexo B1. Descripción del caso de uso [Autenticarse]

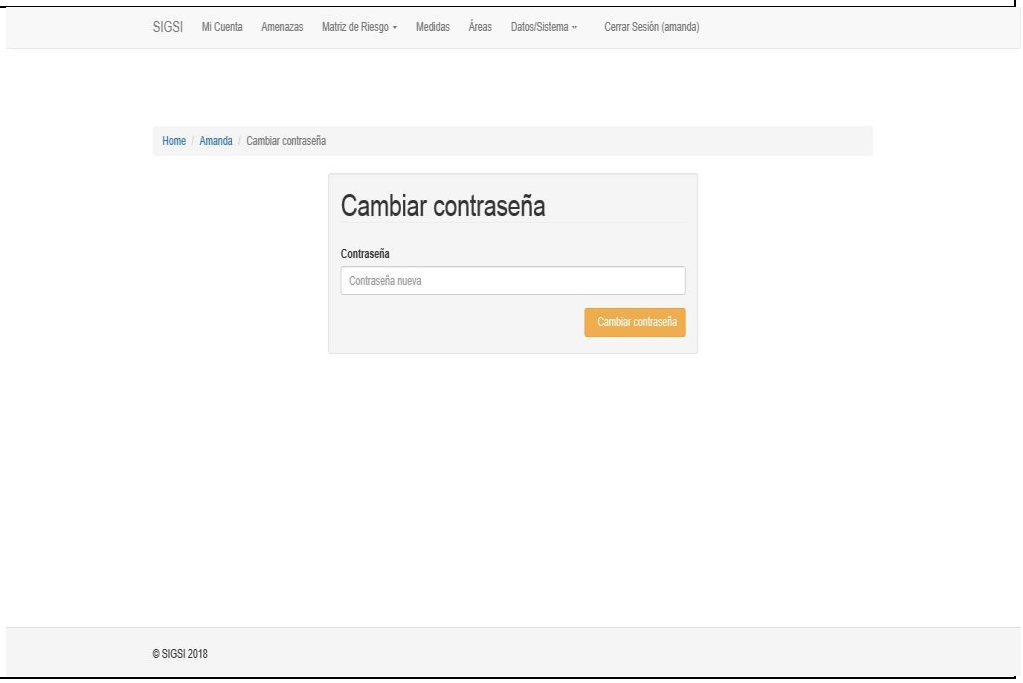
Nombre	Autenticarse
Actores	Usuario (inicia).
Propósito	Verificar la identidad del usuario.
Resumen	El caso de uso se inicia cuando el usuario desea ingresar al sistema. Para ello debe introducir su usuario y contraseña, a continuación, se chequea. Si los datos son correctos el usuario podrá acceder a las opciones del sistema que le corresponden, en el caso de que no lo sean se mostrará un mensaje de error, denegando el acceso.
Referencias	R1
Precondiciones	El usuario debe estar registrado en la base de datos de los usuarios, teniendo un identificador y contraseña.
Post-condiciones	El usuario puede acceder a la información que hay en su sección.
Requisitos Especiales	
Prototipo	

Anexo B2. Descripción del caso de uso [Cerrar sesión]

Nombre	Cerrar Sesión
Actores	Usuario (inicia).
Propósito	El usuario cierre su sesión.
Resumen	El caso de uso se inicia cuando un usuario desea abandonar el sistema. Para que pueda ejecutar esta acción debe haber iniciado sesión antes en el sistema, si ya lo ha hecho puede cerrar su sesión sin ninguna dificultad.
Referencias	R2
Precondiciones	El usuario debe haber iniciado sesión en el sistema.
Post-condiciones	El usuario ya no tiene acceso a las funcionalidades del sistema y puede iniciar sesión cuando lo desee.
Requisitos Especiales	
Prototipo	

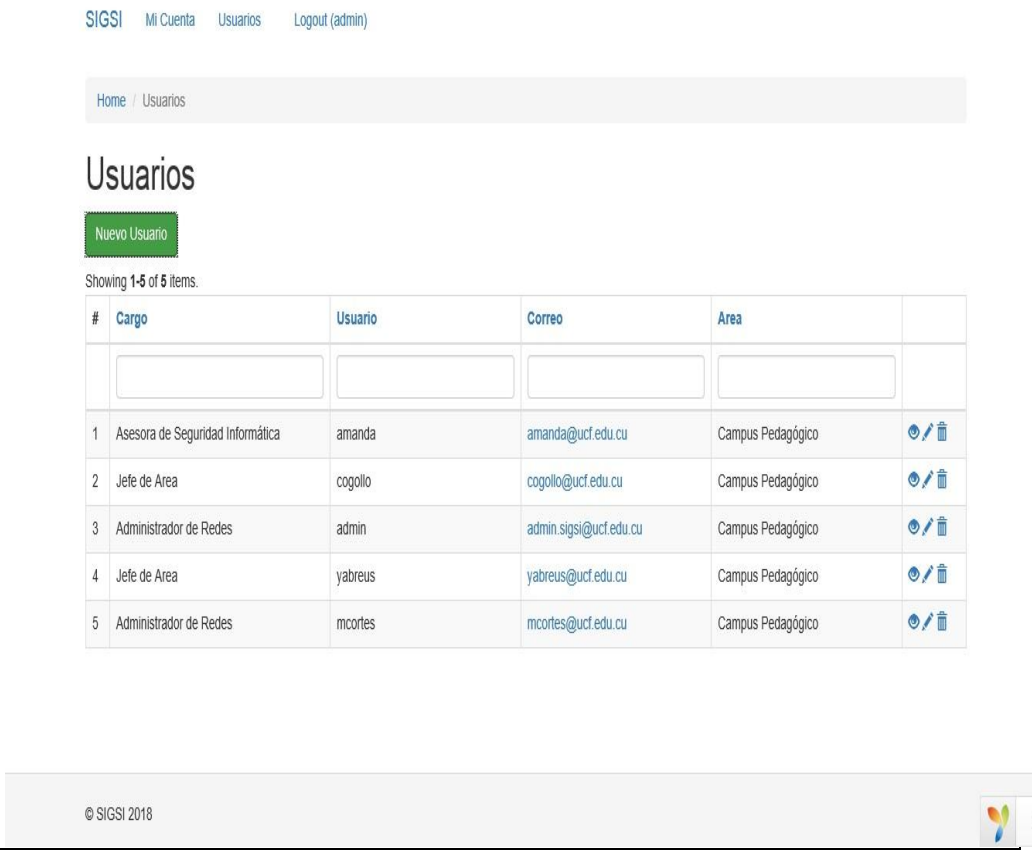
Anexo B3. Descripción del caso de uso [Cambiar contraseña]

Nombre	Cambiar contraseña
Actores	Usuario (inicia).

Propósito	El usuario pueda cambiar su contraseña.
Resumen	El caso de uso se inicia cuando un usuario desea cambiar su contraseña. Para que pueda ejecutar esta acción debe haber iniciado sesión antes en el sistema, si ya lo ha hecho puede acceder al menú Mi Cuenta donde encontrará la opción cambiar contraseña, posibilitando así dicha acción.
Referencias	R3
Precondiciones	El usuario debe haber iniciado sesión en el sistema y debe acceder al menú Mi Cuenta donde encontrará la opción cambiar contraseña.
Post-condiciones	El usuario vuelve al menú Mi Cuenta donde se le muestran sus datos quedando su contraseña actualizada.
Requisitos Especiales	
Prototipo	

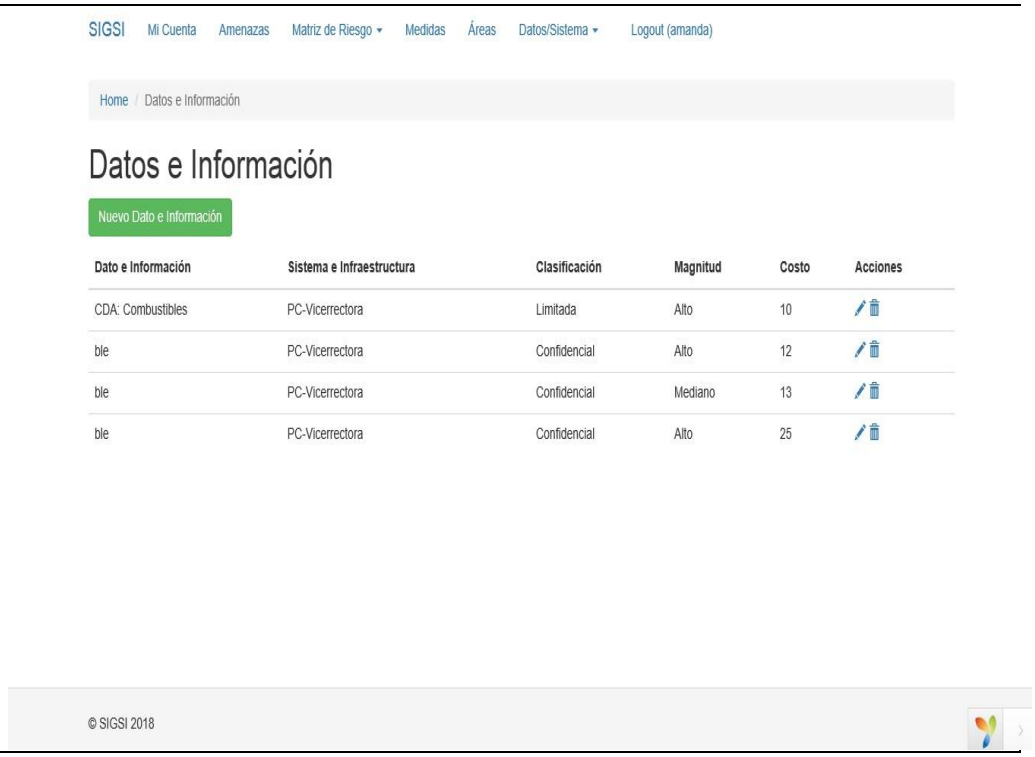
Anexo B4. Descripción del caso de uso [Gestionar usuarios]

Nombre	Gestionar usuarios
Actores	Administrador (inicia).
Propósito	El Administrador gestione los usuarios del sistema.

Resumen	El caso de uso se inicia cuando el Administrador desea gestionar algún usuario, ya sea insertar, modificar, listar o eliminar, para esto el administrador se dirige al botón usuario que aparece en su interfaz donde se le brindan todas esas funcionalidades. El caso de uso termina una vez el administrador modifique o inserte todo lo que considere necesario de los usuarios
Referencias	R4,R5,R6,R7,R8
Precondiciones	El Administrador debe estar autenticado como tal en el sistema para poder gestionar los usuarios del mismo.
Post-condiciones	La información de los usuarios queda modificada
Requisitos Especiales	
Prototipo	

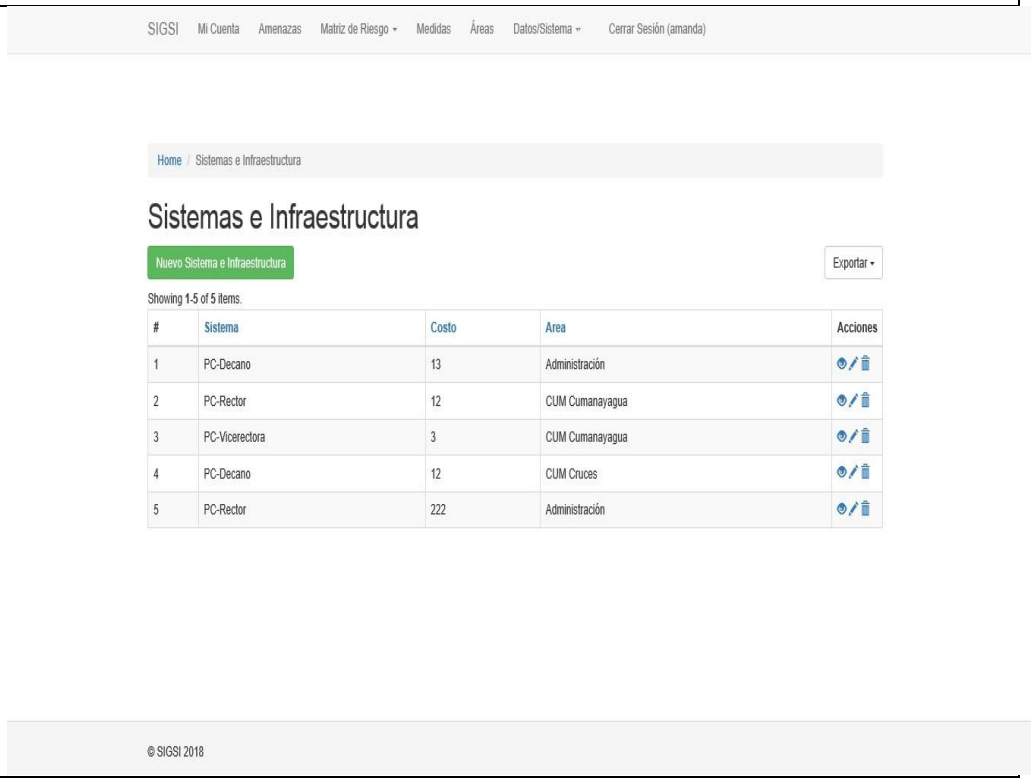
Anexo B5. Descripción del caso de uso [Gestionar Datos e Información]

Nombre	Gestionar Datos e Información
Actores	Jefe de Área y Asesora de SI (inician).
Propósito	El Jefe de Área y la Asesora de SI gestionen la tabla con los datos e información del área o las áreas en dependencia del usuario que realice la acción.
Resumen	El caso de uso se inicia cuando un jefe de área desea gestionar los datos e información referente su área, o la asesora de SI desea gestionar los datos e información de todas las áreas, ya sea mostrar, actualizar o eliminar. Para esto ambos usuarios se dirigen a la opción datos _sistema que aparecen en sus respectivas interfaces y seleccionan la opción datos o información. El caso de uso termina cuando cualquiera de estos dos usuarios actualizó o añadió información referente a los datos o información.
Referencias	R9,R10,R11,R12
Precondiciones	El jefe de área o la asesora de SI deben haberse autenticado en el sistema como tal.
Post-condiciones	Queda actualizada la base de datos del sistema con los datos insertados de los datos e información, guardados los cambios efectuados sobre los existentes o si se elimina alguno, en caso de haber elegido esta opción.
Requisitos Especiales	

Prototipo	

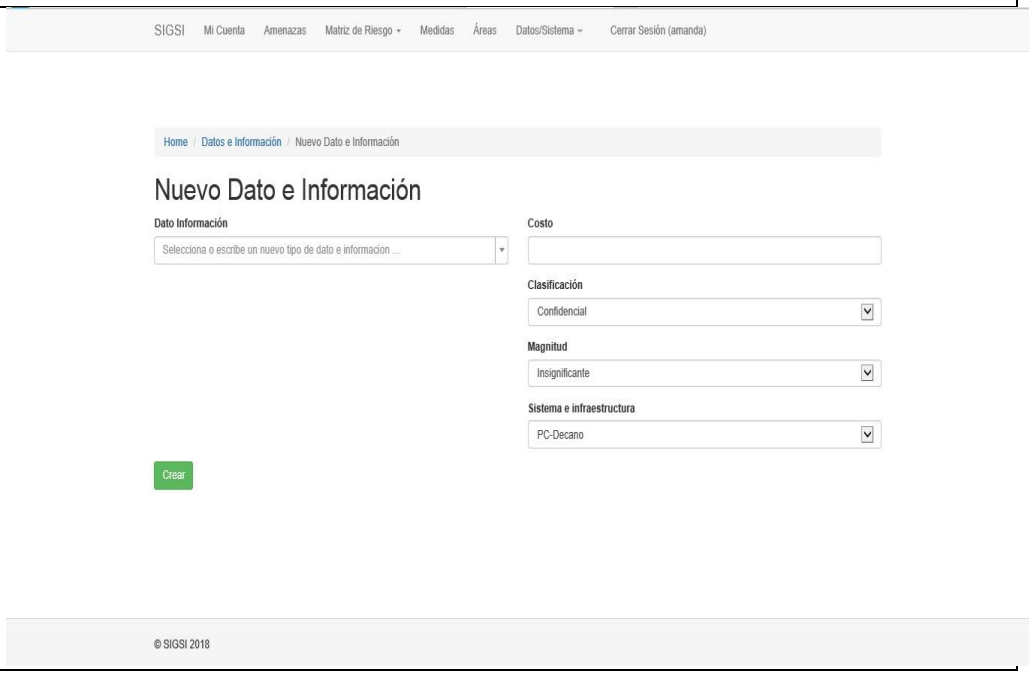
Anexo B6. Descripción del caso de uso [Gestionar Infraestructura]

Nombre	Gestionar Infraestructura
Actores	Jefe de Área y Asesora de SI (inician).
Propósito	El Jefe de Área y la Asesora de SI gestión en la tabla con la infraestructura del área o las áreas en dependencia del usuario que realice la acción.
Resumen	El caso de uso se inicia cuando un jefe de área desea gestionar la infraestructura referente su área, o la asesora de SI desea gestionar la infraestructura de todas las áreas, ya sea mostrar, actualizar o eliminar. Para esto ambos usuarios se dirigen a la opción datos _sistema que aparecen en sus respectivas interfaces y seleccionan la opción Sistema e infraestructura. El caso de uso termina cuando cualquiera de estos dos usuarios actualizó o añadió información referente a la infraestructura.
Referencias	R13,R14,R15,R16

Precondiciones	El jefe de área o la asesora de SI deben haberse autenticado en el sistema como tal.
Post-condiciones	Queda actualizada la base de datos del sistema con los datos insertados de la infraestructura, guardados los cambios efectuados sobre las existentes o si se elimina alguna, en caso de haber elegido esta opción.
Requisitos Especiales	
Prototipo	

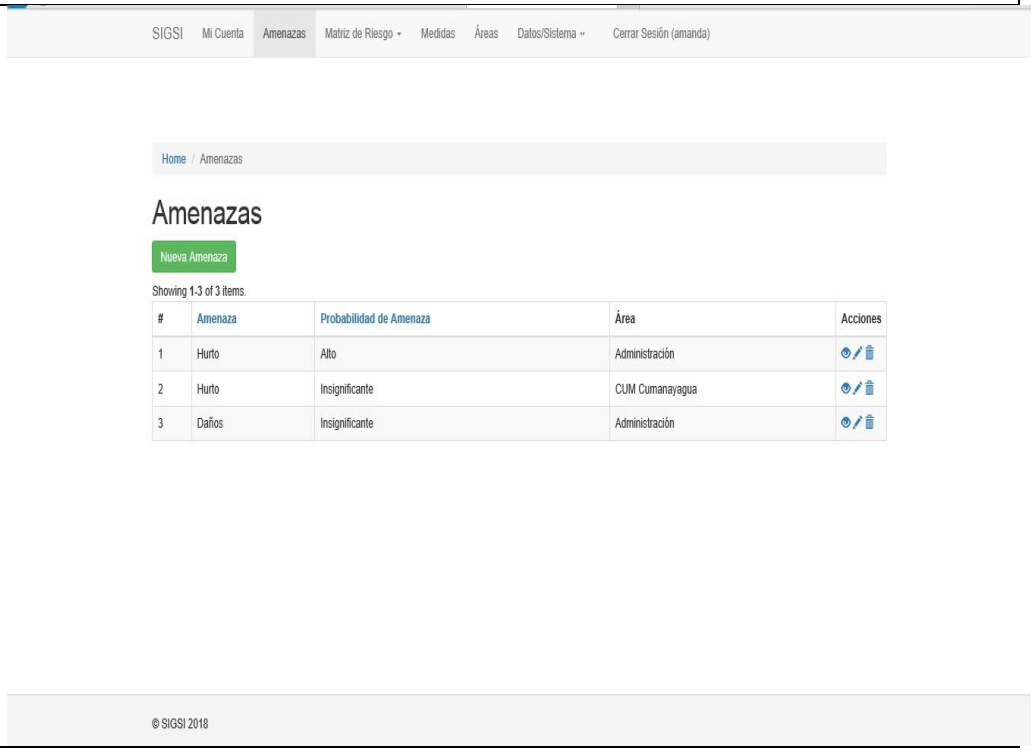
Anexo B7. Descripción del caso de uso [Relacionar infraestructura con datos e información]

Nombre	Relacionar infraestructura con datos e información
Actores	Jefe de Área, Asesora de SI (inician).
Propósito	Crear una relación entre un Dato o Información y un Sistema e Infraestructura propiciando así que un Jefe de Área o la Asesora de SI no puedan crear un dato e Información sin hacerle corresponder una Infraestructura

Resumen	El caso de uso se inicia cuando un jefe de área o la Asesora de SI desea crear un Dato o Información. Para esto ambos usuarios se dirigen a la opción datos _sistema que aparecen en sus respectivas interfaces y seleccionan la opción Dato o Información, donde para poder añadir un nuevo Dato es necesario hacerle corresponder una infraestructura. Terminando así el caso de uso.
Referencias	R17
Precondiciones	El jefe de área o la asesora de SI deben haberse autenticado en el sistema como tal y debe estar creado un sistema e infraestructura.
Post-condiciones	El jefe de área o la asesora de SI pueden crear un nuevo Dato o Información.
Requisitos Especiales	
Prototipo	

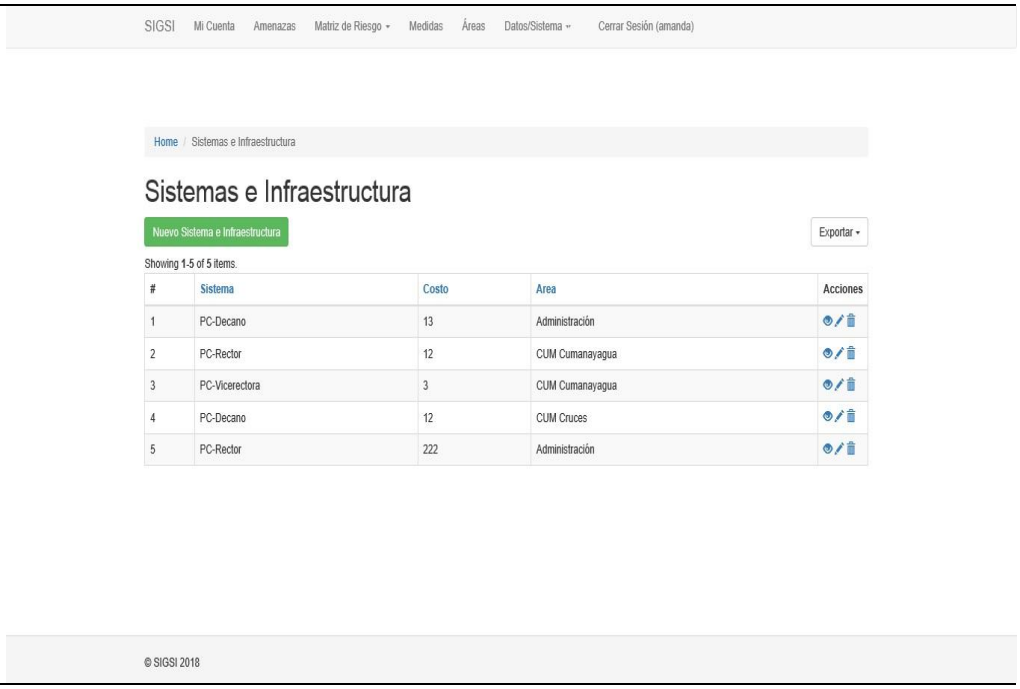
Anexo B8. Descripción del caso de uso [Gestionar Amenazas]

Nombre	Gestionar Amenazas
Actores	Administrador de Red y Asesora de SI (inician).
Propósito	El Administrador de Red gestione la tabla con las amenazas detectadas y la Asesora de SI gestione las amenazas de todas la

	áreas
Resumen	El caso de uso se inicia cuando el administrador de red o la asesora de SI desean gestionar las amenazas, ya sea mostrar, actualizar o eliminar. Para esto ambos usuarios poseen en sus respectivas interfaces la opción amenazas, donde pueden gestionar dichas amenazas. El caso de uso termina una vez el administrador de red o la asesora de SI modificaron la información referente a las amenazas en el sistema
Referencias	R18,R19,R20,R21
Precondiciones	El administrador de redo la asesora de SI deben haberse autenticado en el sistema como tal.
Post-condiciones	Queda actualizada la base de datos del sistema con los datos insertados de las amenazas, guardados los cambios efectuados sobre las existentes o si se elimina alguna, en caso de haber elegido esta opción.
Requisitos Especiales	
Prototipo	

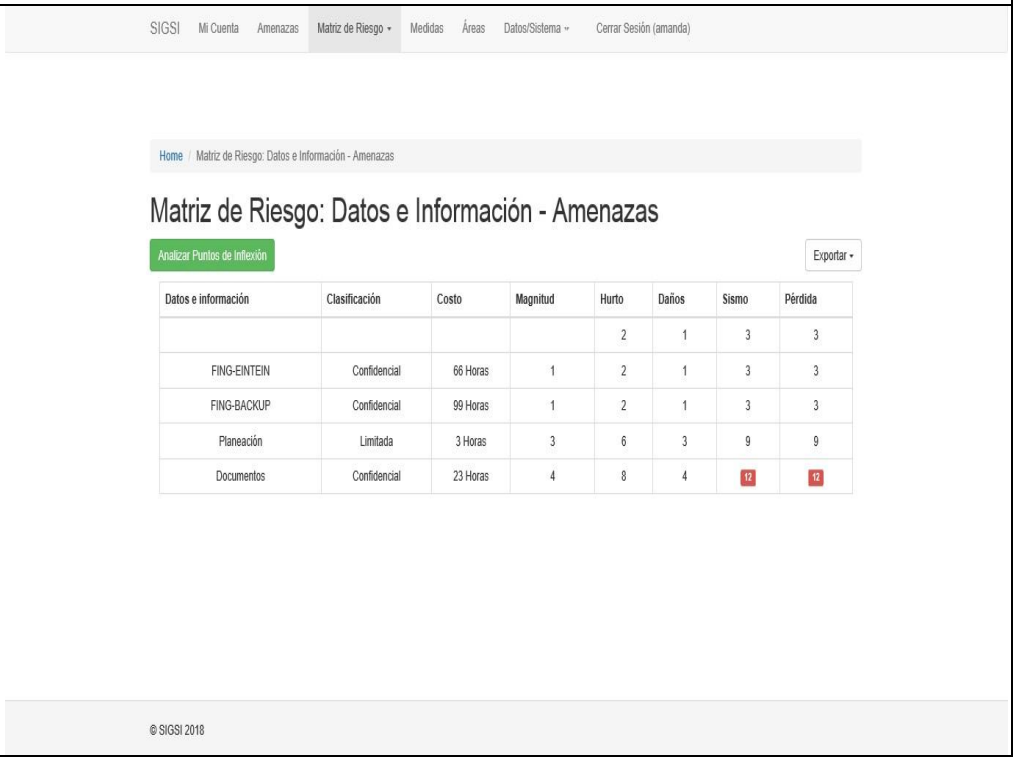
Anexo B9. Descripción del caso de uso [Visualizar descripción de los componentes de la Red]

Nombre	Visualizar descripción de los componentes de la Red
Actores	Asesora de SI (inician).
Propósito	La Asesora de SI pueda visualizar a que área pertenece cada infraestructura
Resumen	El caso de uso se inicia cuando la asesora de SI desea visualizar a que área pertenece cada infraestructura. Para ello la asesora se dirige a la opción datos _sistema que aparecen en su interfaz y seleccionan la opción Sistema e Infraestructura, donde se le mostrará cada sistema con el área al que pertenece. Terminando así el caso de uso.
Referencias	R22,R23
Precondiciones	La Asesora de SI debe haberse autenticado en el sistema como tal y debe existir como mínimo un sistema e infraestructura creado de lo contrario no se podrá visualizar nada.
Post-condiciones	La Asesora de SI puede acceder a cualquier otra opción dentro de su interfaz en el sistema.
Requisitos Especiales	

Prototipo	

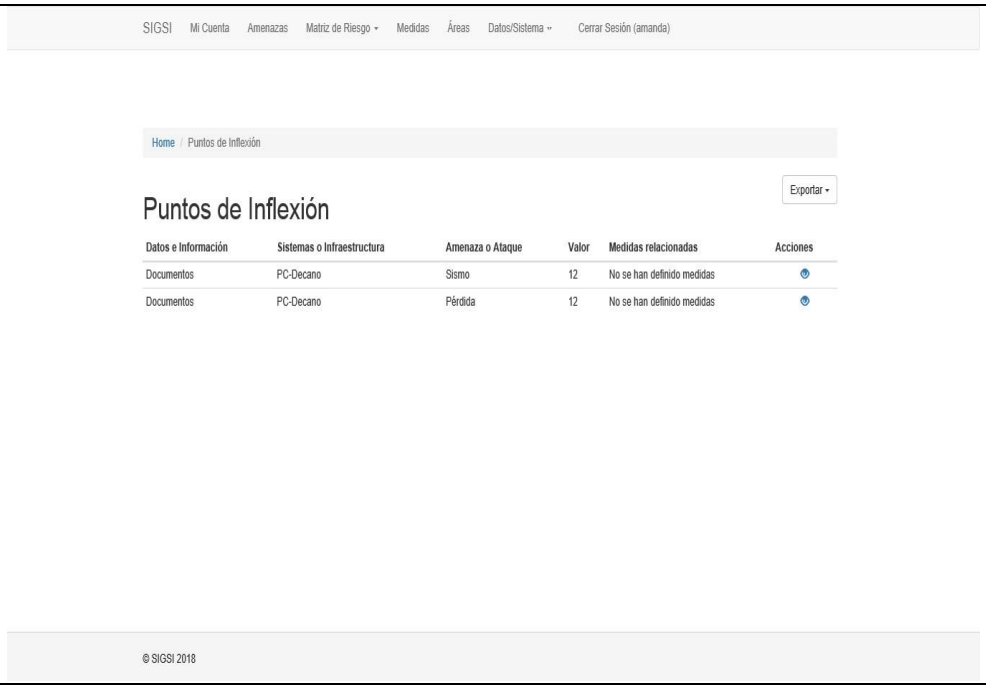
Anexo B10. Descripción del caso de uso [Visualizar Matriz]

Nombre	Visualizar Matriz
Actores	Administrador de Red, Asesora de SI, Jefe de Área (inician).
Propósito	Que cualquiera de los usuarios del sistema, ya sea el jefe de área, el administrador de Red o la asesora de SI, exceptuando al administrador del sistema, puedan visualizar la matriz de riesgos
Resumen	El caso de uso se inicia cuando cualquiera de los usuarios del sistema, ya sea el jefe de área, el administrador de Red o la asesora de SI, exceptuando al administrador del sistema, se dirige a la opción Matriz de Riesgo en cualquiera de sus respectivas cesiones, donde seleccionando la opción Datos e Información_Amenaza pueden visualizar la matriz de riesgos con los datos correspondiente a cada usuario en caso de ser jefe de área o administrador de red y general en el caso de la asesora. Terminando así el caso de uso.
Referencias	R24,R25
Precondiciones	Cualquiera de estos usuarios mencionados debe haberse autenticado en el sistema como tal y debe tener amenazas, datos y

	sistemas añadidos de lo contrario no se visualizará nada.
Post-condiciones	Estos usuarios pueden acceder a cualquier otra opción dentro de su interfaz en el sistema
Requisitos Especiales	
Prototipo	

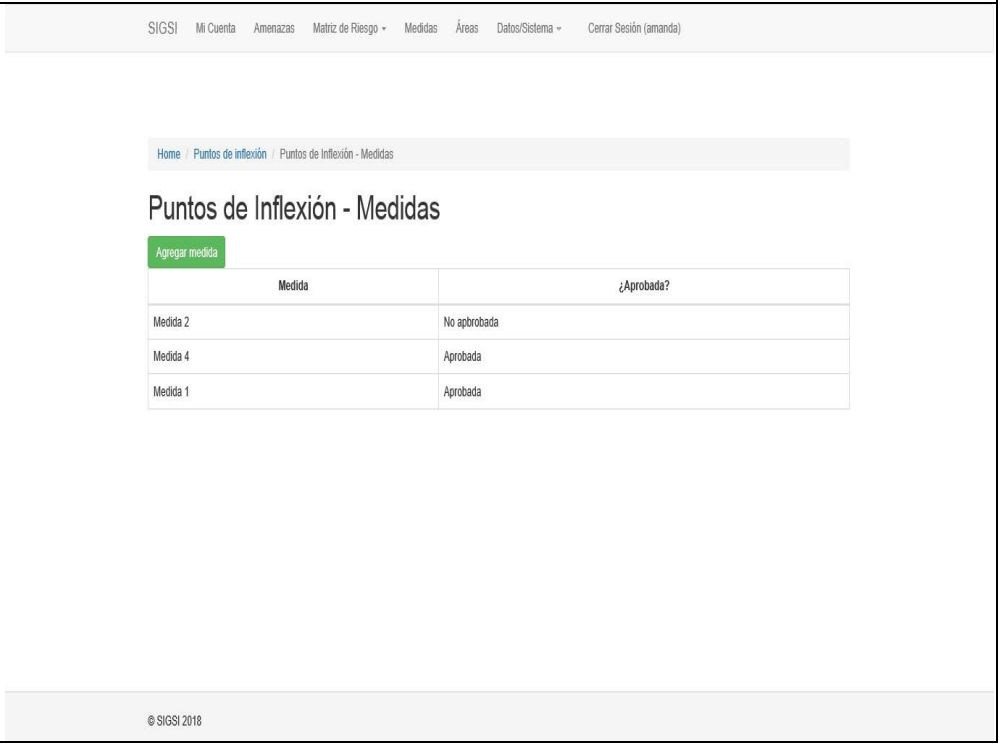
Anexo B11. Descripción del caso de uso [Analizar Puntos de Inflexión]

Nombre	Analizar Puntos de Inflexión
Actores	Asesora de SI (inician).
Propósito	Que la asesora de SI pueda analizar cada punto de inflexión, pudiendo observar el conjunto de datos que le corresponde a dicho punto
Resumen	El caso de uso se inicia cuando la asesora de SI necesita analizar cada punto de inflexión. Para esto la asesora se dirige a la opción Matriz de Riesgo donde seleccionando la opción Datos e Información_Amenaza puede visualizar la matriz de riesgos, y aquí seleccionando la opción analizar puntos de inflexión puede ver los

	datos de cada punto como por ejemplo el dato o información, la infraestructura y la amenaza. Terminando así el caso de uso.
Referencias	R26,R37
Precondiciones	La Asesora de SI debe haberse autenticado en el sistema como tal, debe haberse generado la matriz de riesgos y detectado puntos de inflexión.
Post-condiciones	La Asesora de SI puede proceder a realizar cualquier otra acción dentro de su interfaz.
Requisitos Especiales	
Prototipo	

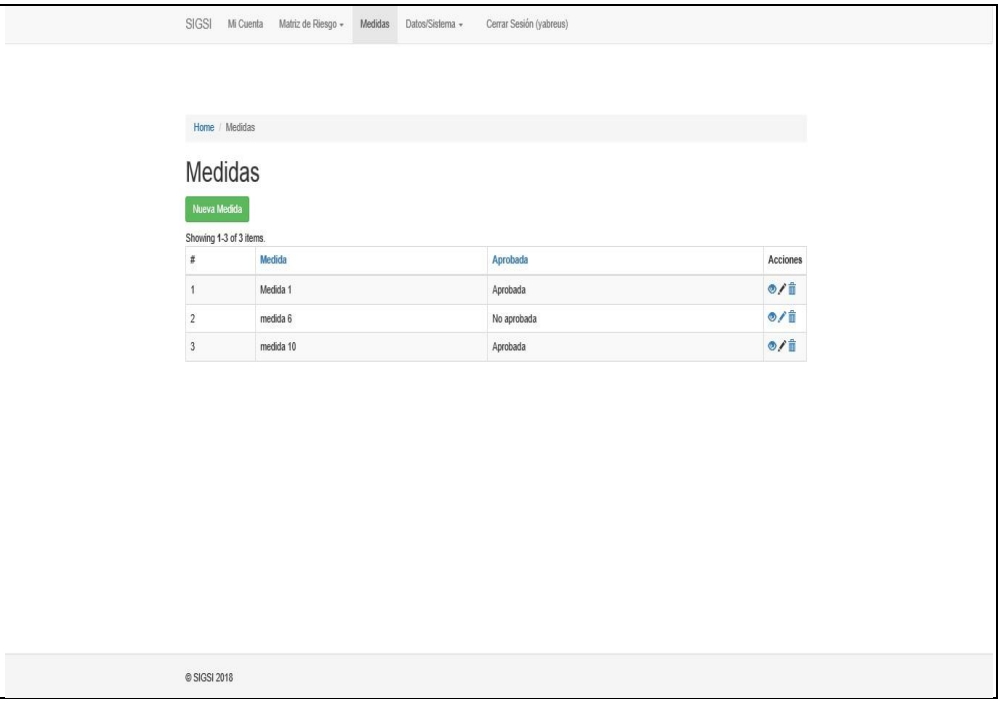
Anexo B12. Descripción del caso de uso [Relacionar puntos de inflexión con medidas]

Nombre	Relacionar puntos de inflexión con medidas
Actores	Asesora de SI (inicia).
Propósito	Que la asesora de SI pueda analizar cada punto de inflexión, pudiendo añadir un conjunto de medidas a cada punto
Resumen	El caso de uso se inicia cuando la asesora de SI necesita añadir medidas a cada punto de inflexión. Para esto la asesora se dirige a

	la opción Matriz de Riesgo donde seleccionando la opción Datos e Información_Amenaza puede visualizar la matriz de riesgos, y aquí seleccionando la opción analizar puntos de inflexión puede ver los datos de cada punto como por ejemplo el dato o información, la infraestructura y la amenaza. Una vez aquí para añadir medidas selecciona la opción ver que le permite esta funcionalidad Terminando así el caso de uso.
Referencias	R28,R29
Precondiciones	La Asesora de SI debe haberse autenticado en el sistema como tal, debe haberse generado la matriz de riesgos y detectado puntos de inflexión.
Post-condiciones	La Asesora de SI puede proceder a realizar cualquier otra acción dentro de su interfaz.
Requisitos Especiales	
Prototipo	

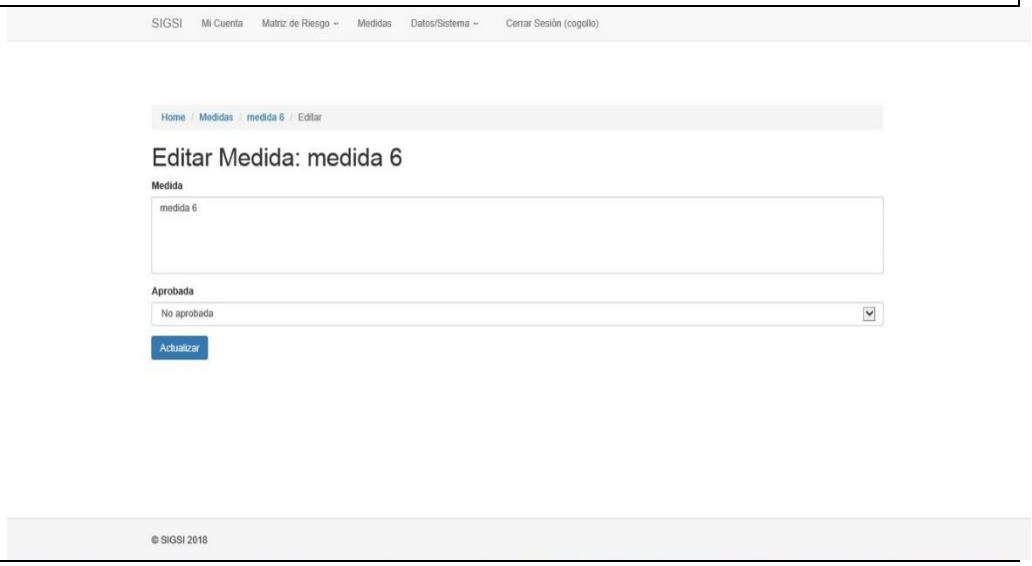
Anexo B13. Descripción del caso de uso [Gestionar medidas]

Nombre	Gestionar medidas
Actores	Asesora de SI, Jefe de Área (inicia).
Propósito	La asesora de SI y los jefes de área pueda agregar, modificar, listar y ver las medidas para cada punto de inflexión
Resumen	El caso de uso se inicia cuando la asesora de SI necesita crear un conjunto de medidas a tener en cuenta para con un punto de inflexión, a su vez puede modificar, ver y listar dichas medidas, los jefes de área pueden analizar estas medidas, realizarle modificaciones, listarlas e incluso crear alguna.
Referencias	R30,R31,R32,R33
Precondiciones	La asesora de SI o un jefe de área deben haberse autenticado en el sistema como tal, debe haberse generado la matriz de riesgos y detectado puntos de inflexión, además se le deben haber añadido medidas a dichos puntos.
Post-condiciones	El jefe de área o la Asesora de SI pueden proceder a realizar cualquier otra acción dentro de su interfaz.
Requisitos Especiales	

Prototipo	

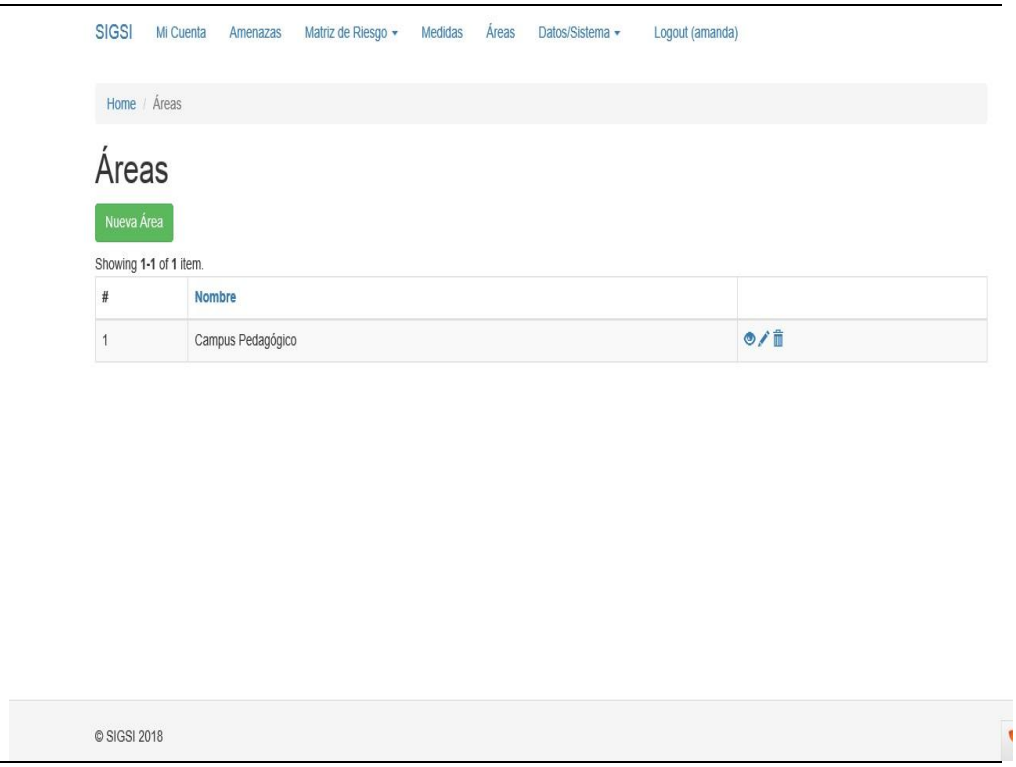
Anexo B14. Descripción del caso de uso [Aprobar Medidas]

Nombre	Aprobar Medidas
Actores	Jefe de Área (inicia).
Propósito	Un jefe de área puede aprobar este conjunto de medidas para con estas elaborar el plan de seguridad informática
Resumen	El caso de uso se inicia cuando un jefe de área específico el cual será el rector de la UCF necesita aprobar las medidas añadidas por la asesora de seguridad y los jefes de área.
Referencias	R34
Precondiciones	Este jefe de área debe haberse autenticado en el sistema como tal, debe haberse generado la matriz de riesgos y detectado puntos de inflexión, además se le deben haber añadido medidas a dichos puntos
Post-condiciones	El jefe de área puede proceder a realizar cualquier otra acción dentro de su interfaz.

Requisitos Especiales	
Prototipo	

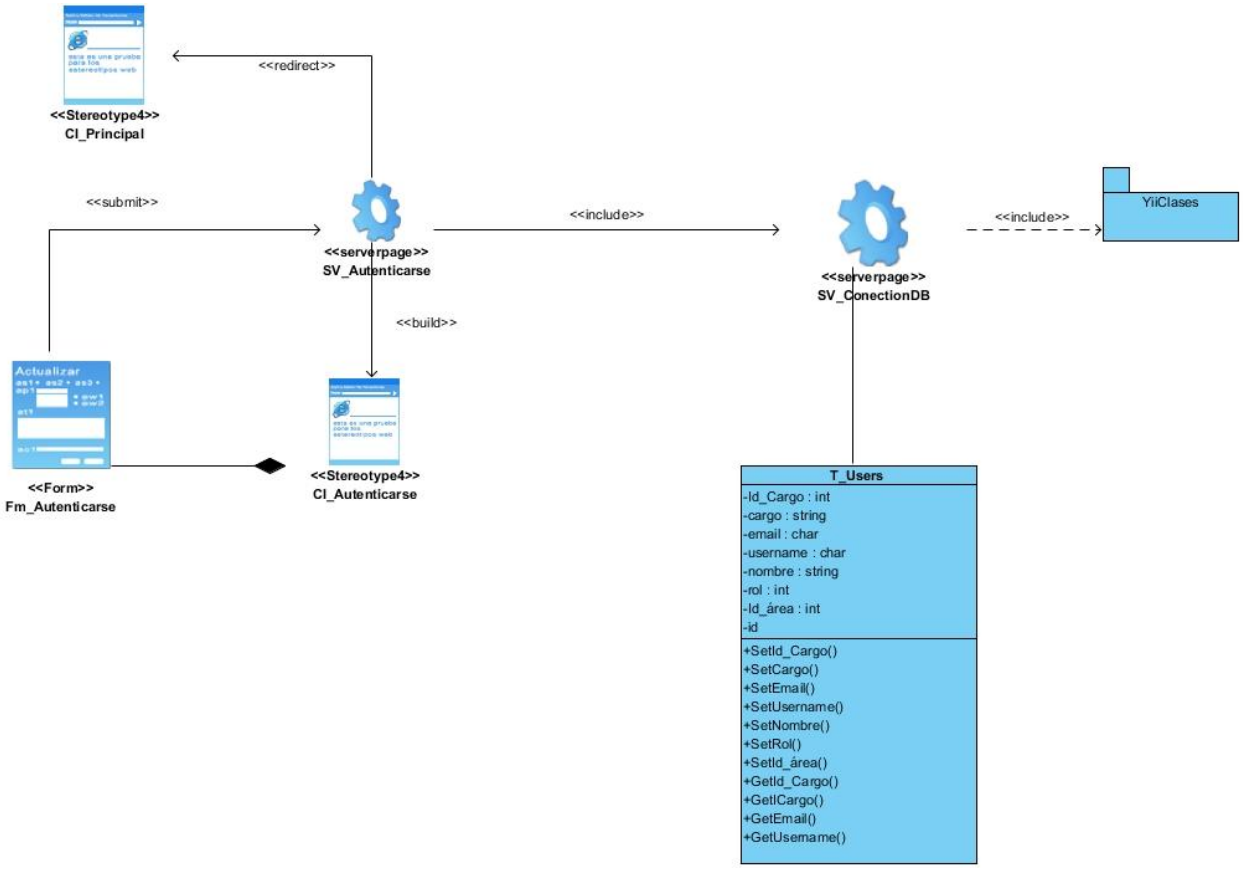
Anexo B15. Descripción del caso de uso [Gestionar Áreas]

Nombre	Gestionar Áreas
Actores	Asesora de SI (inicia).
Propósito	La Asesora de SI pueda gestionar las áreas con las que contará el sistema
Resumen	El caso de uso se inicia cuando la asesora de SI desean gestionar las áreas, ya sea mostrar, listar, actualizar o eliminar. Para esto poseen en su interfaz la opción áreas, donde pueden gestionar las mismas. El caso de uso termina una vez la asesora de SI modificó la información referente a las áreas en el sistema
Referencias	R35,R36,R37,R38
Precondiciones	La asesora de SI debe haberse autenticado en el sistema como tal.
Post-condiciones	La Asesora de SI puede proceder a realizar cualquier otra acción dentro de su interfaz.
Requisitos Especiales	

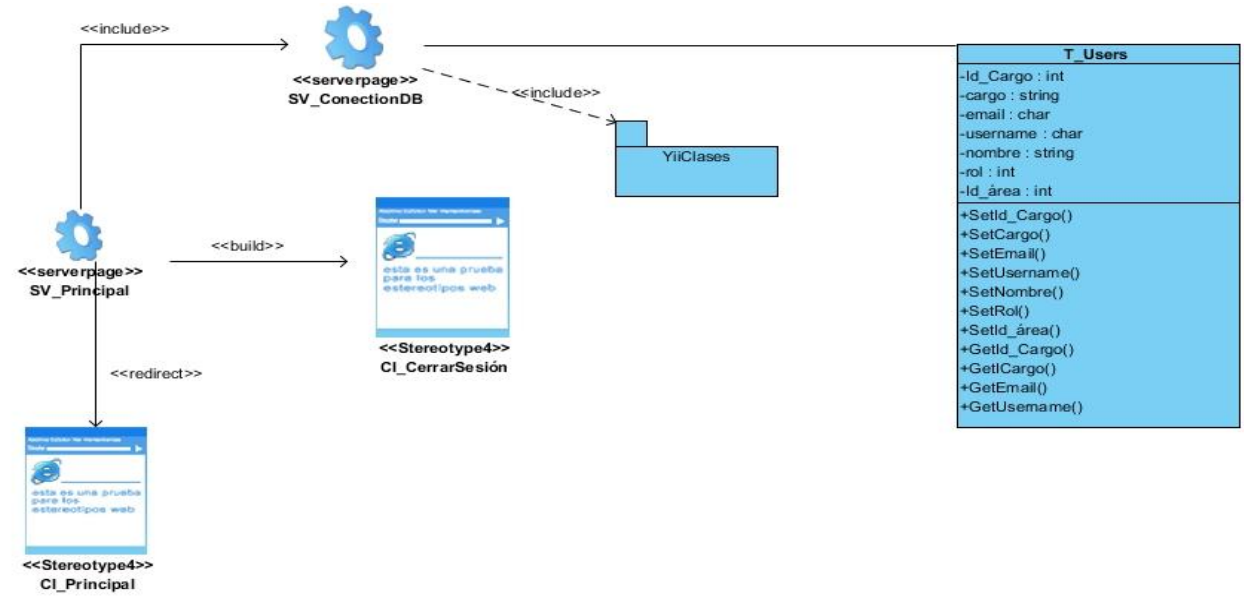
Prototipo	

Anexo C-Diagramas de diseño de clases web

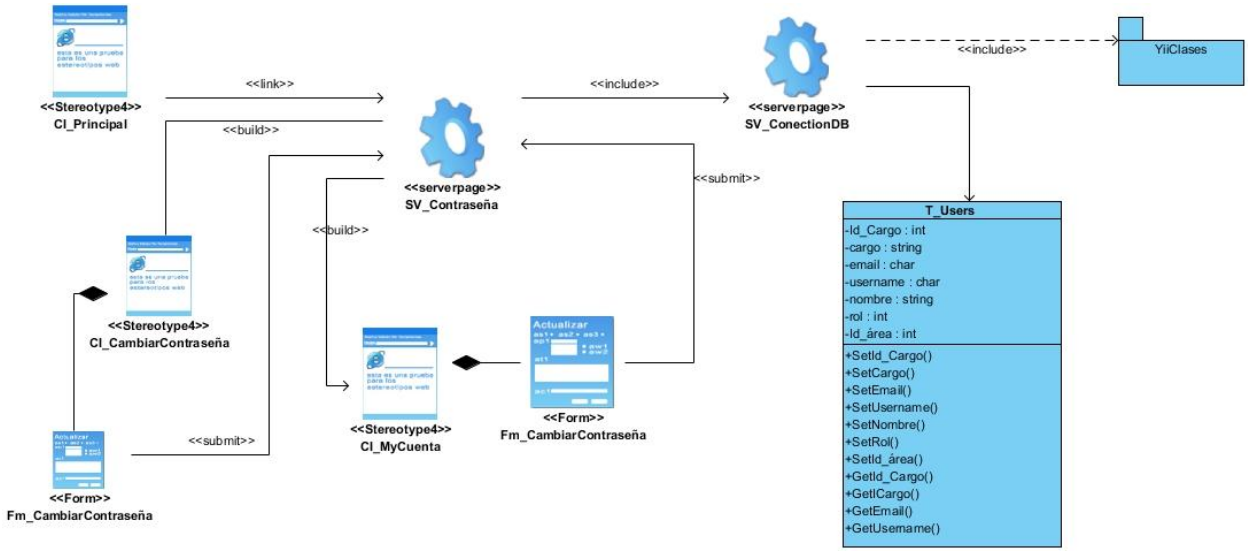
Anexo C1. Autenticarse



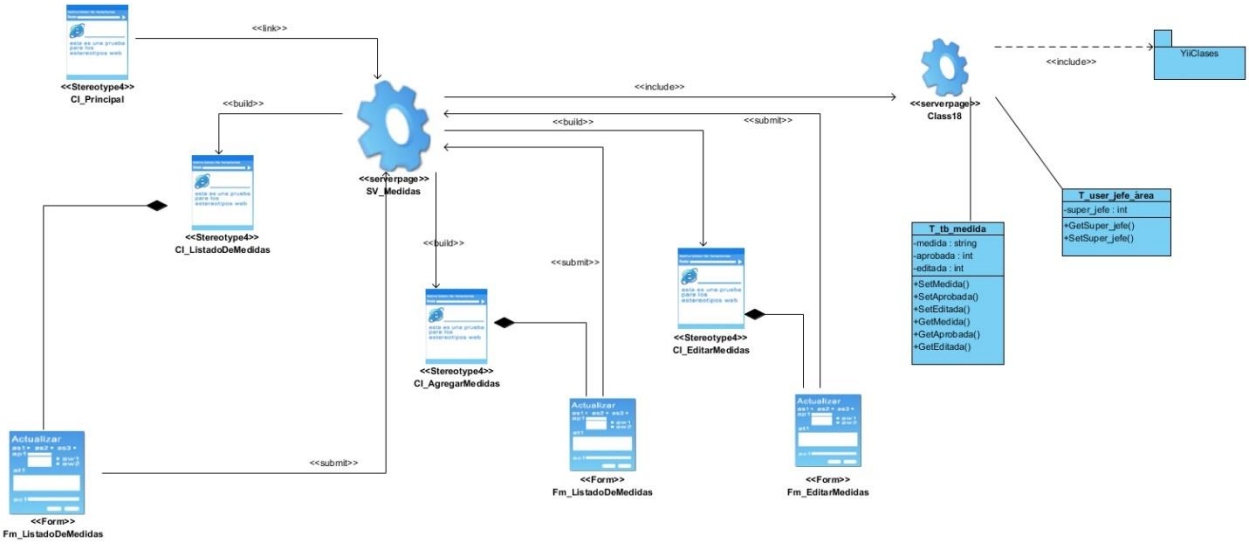
Anexo C2. Cerrar Sesión



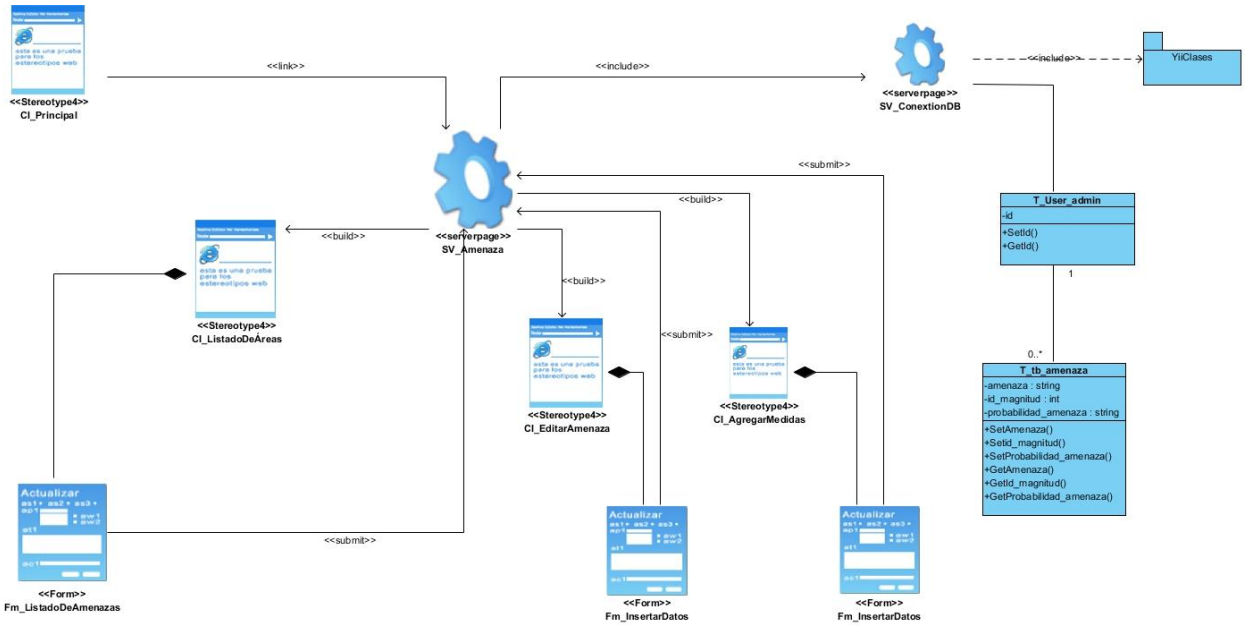
Anexo C3. Cambiar Contraseña



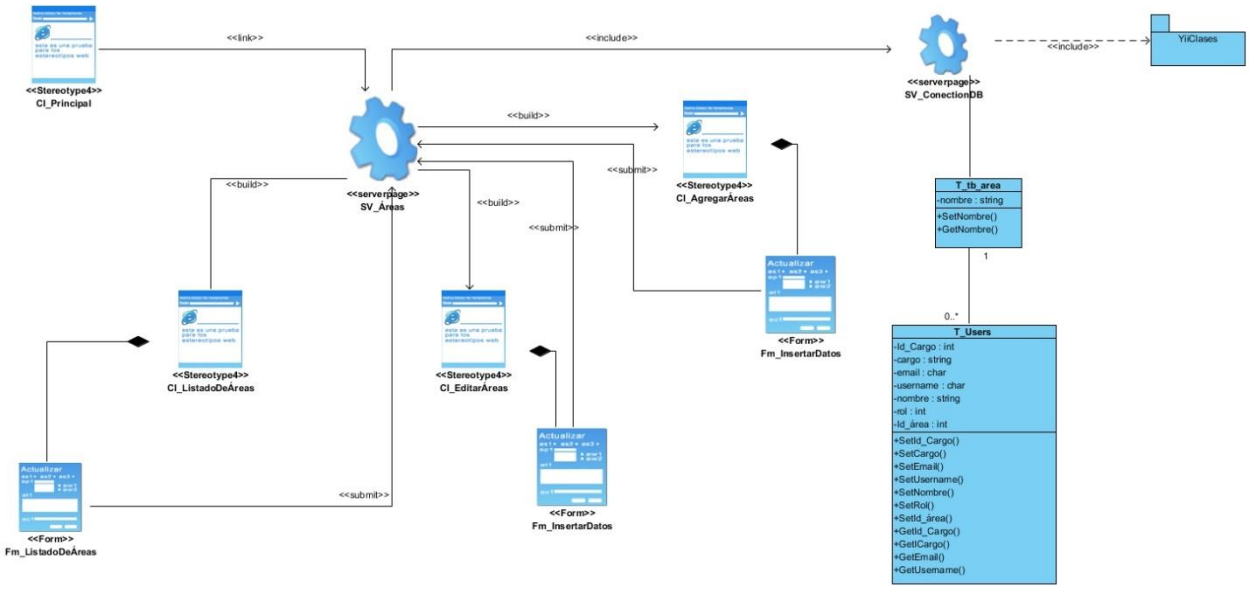
Anexo C4. Aprobar Medidas



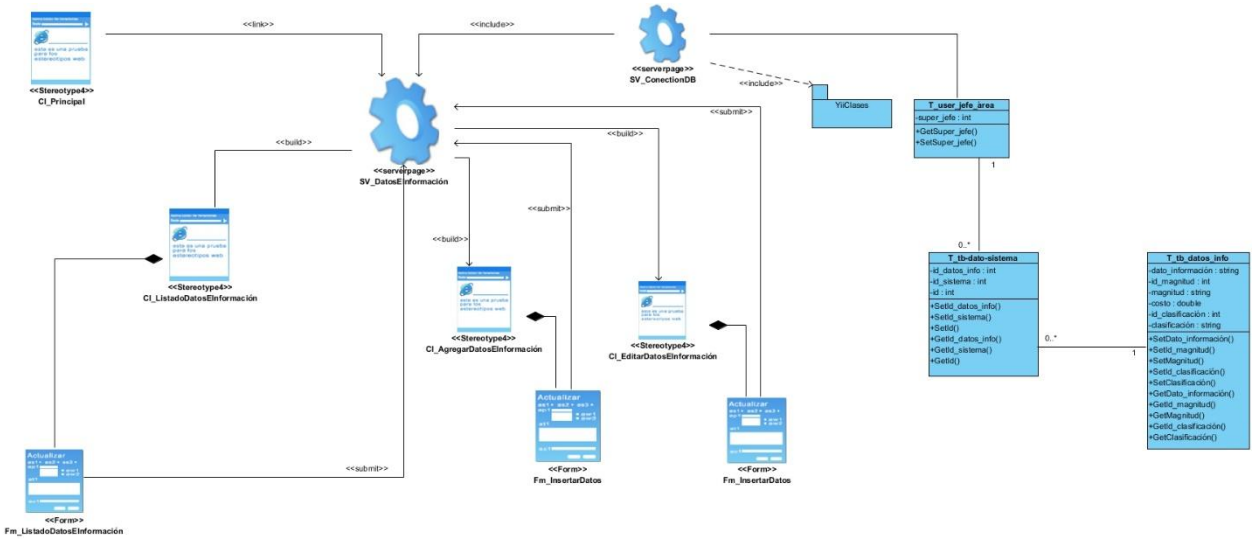
Anexo C5. Gestionar Amenazas



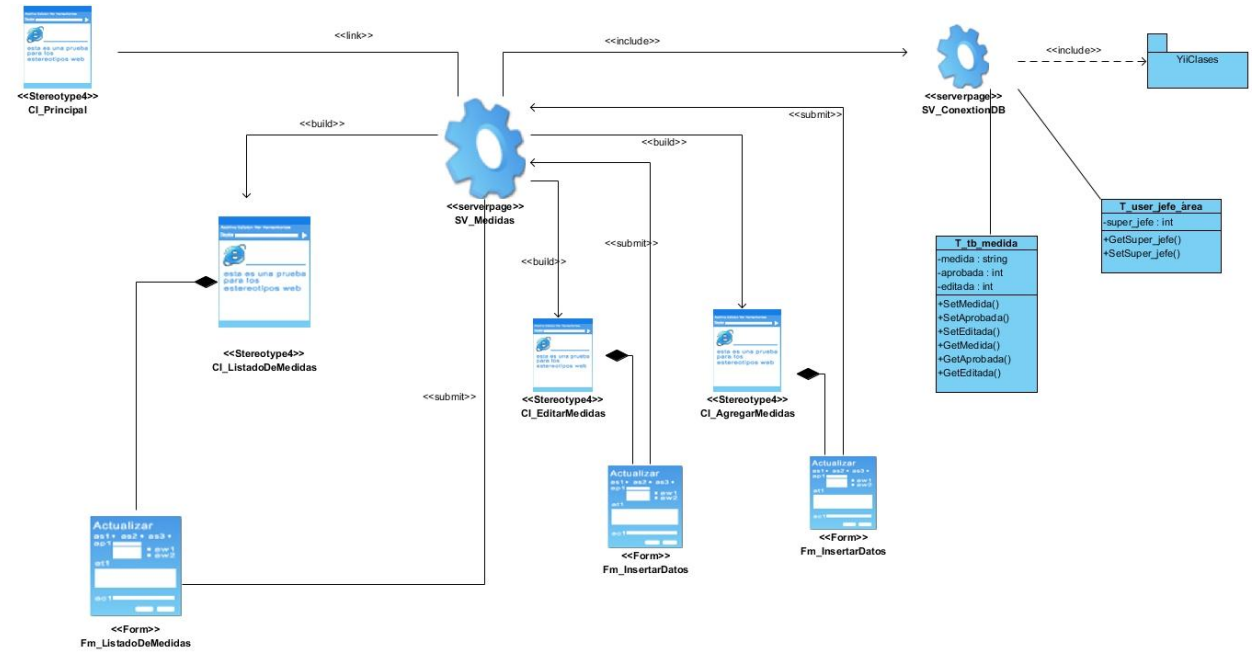
Anexo C6. Gestionar Áreas



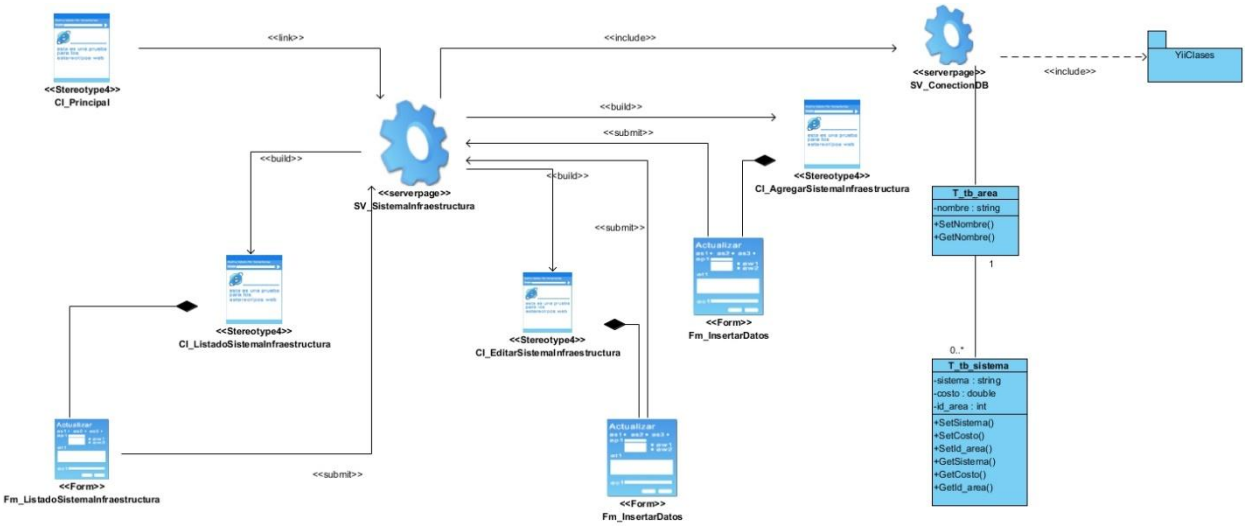
Anexo C7. Gestionar Datos e Información



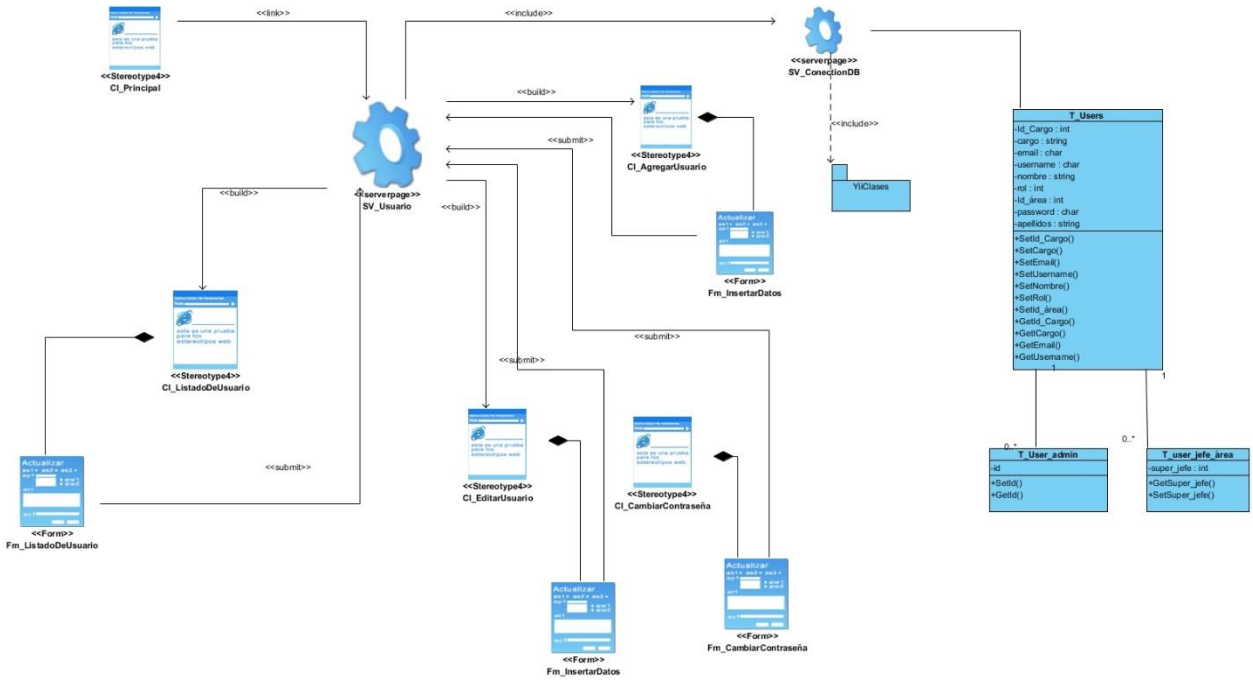
Anexo C8. Gestionar Medidas



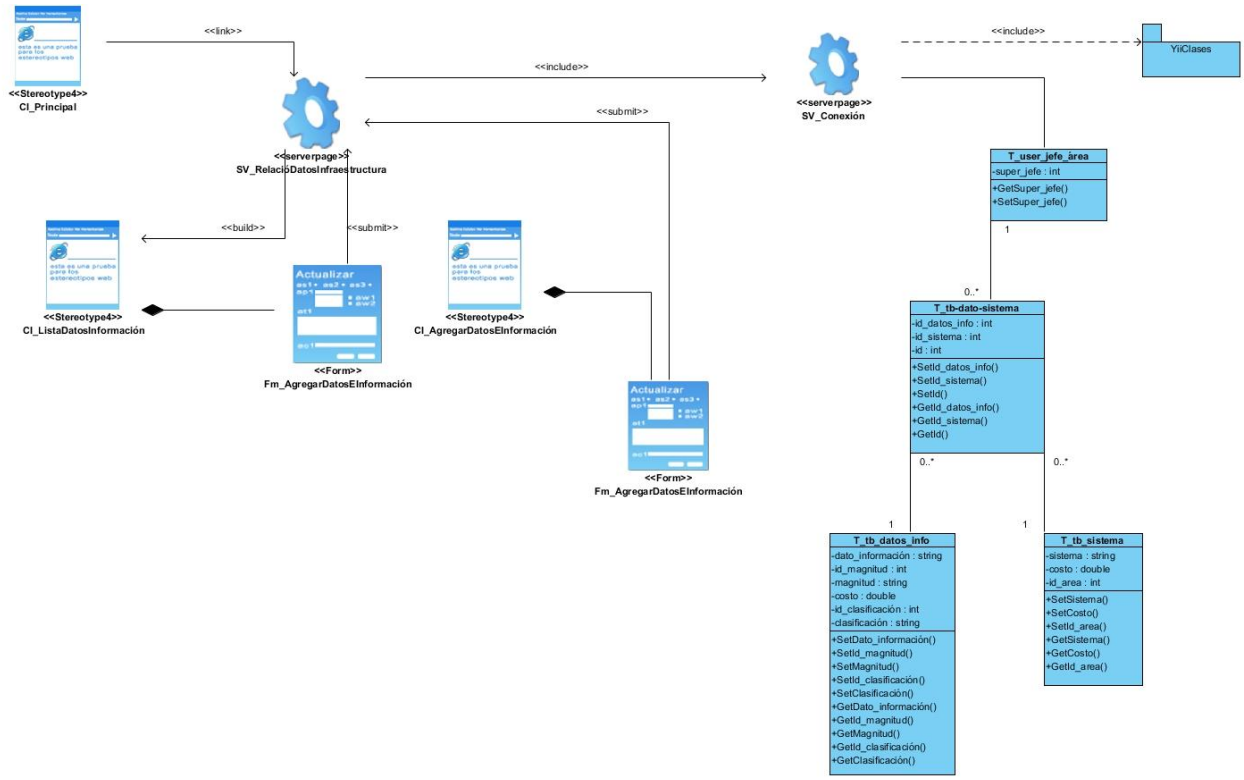
Anexo C9. Gestionar Sistema e Infraestructura



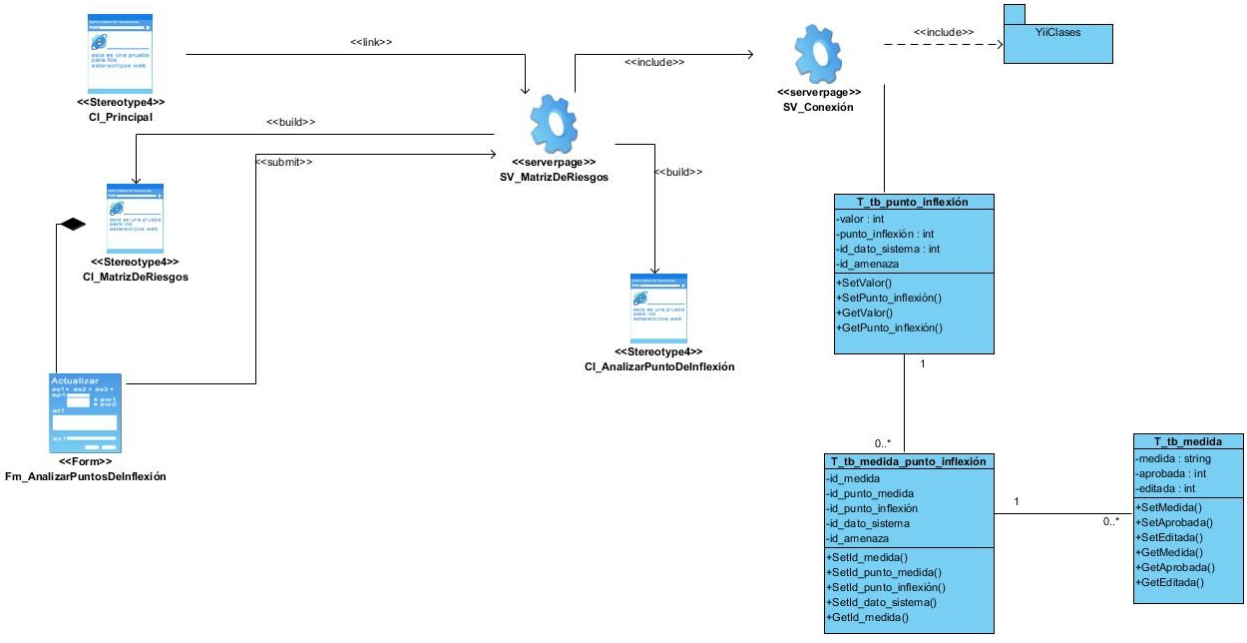
Anexo C10. Gestionar Usuarios



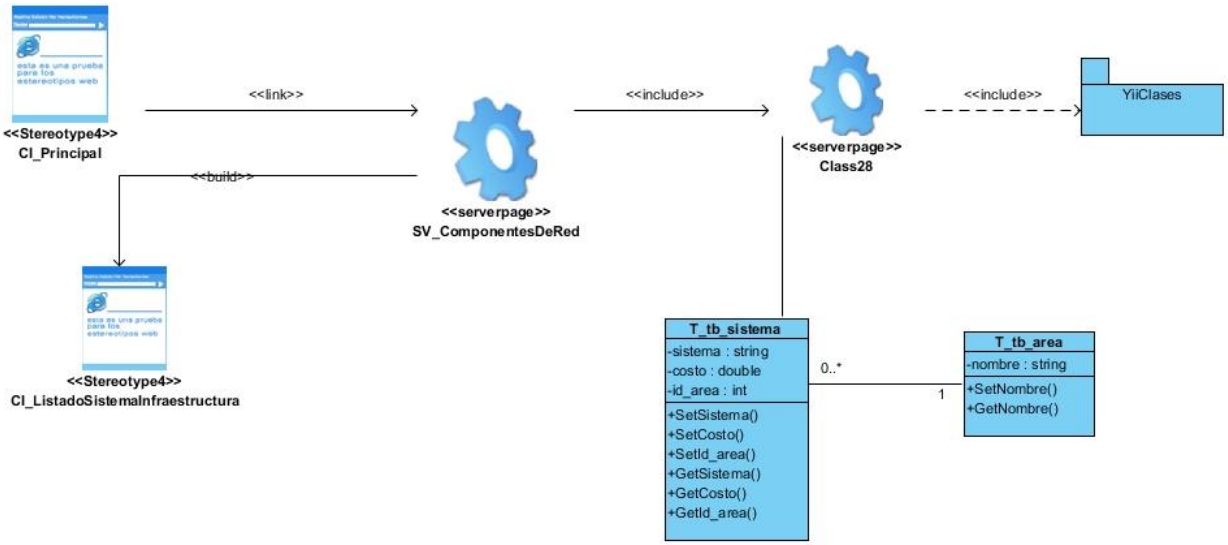
Anexo C11. Relacionar Datos e información con sistema e infraestructura



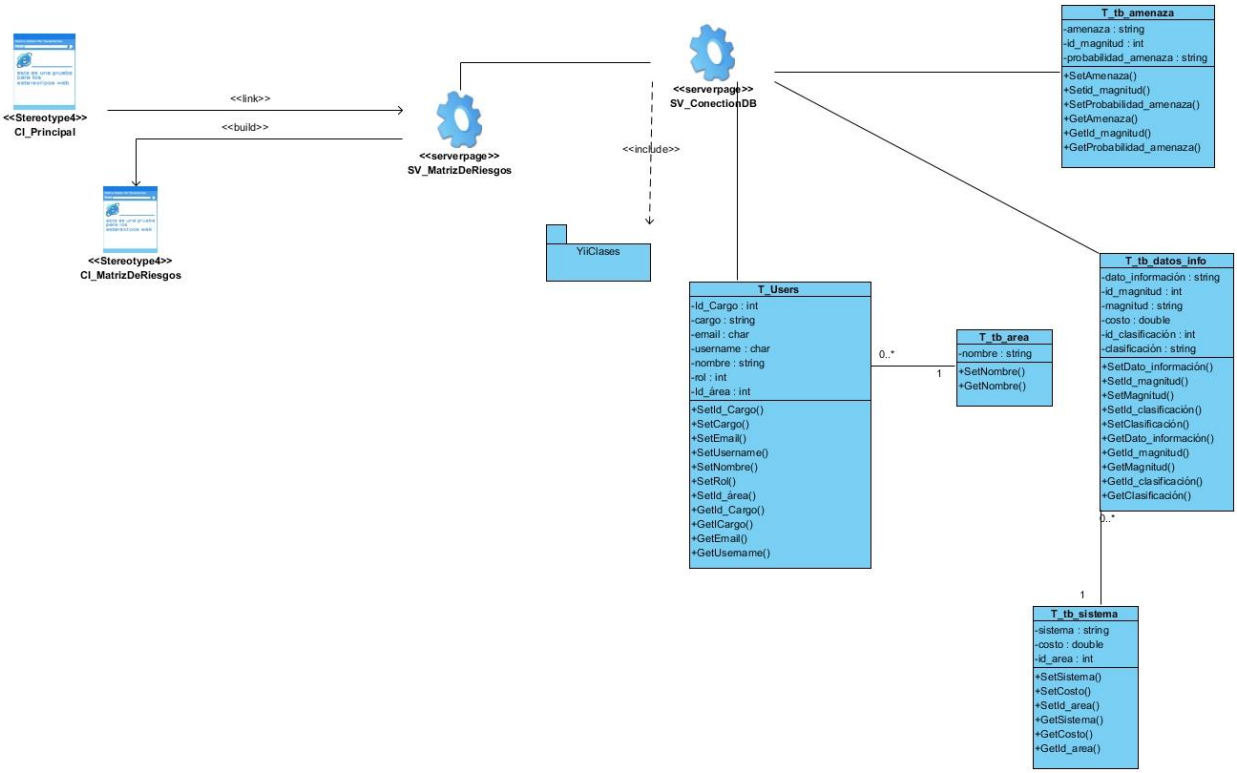
Anexo C12. Relacionar Puntos de inflexión con Medidas



Anexo C13. Visualizar descripción de los componentes de la red

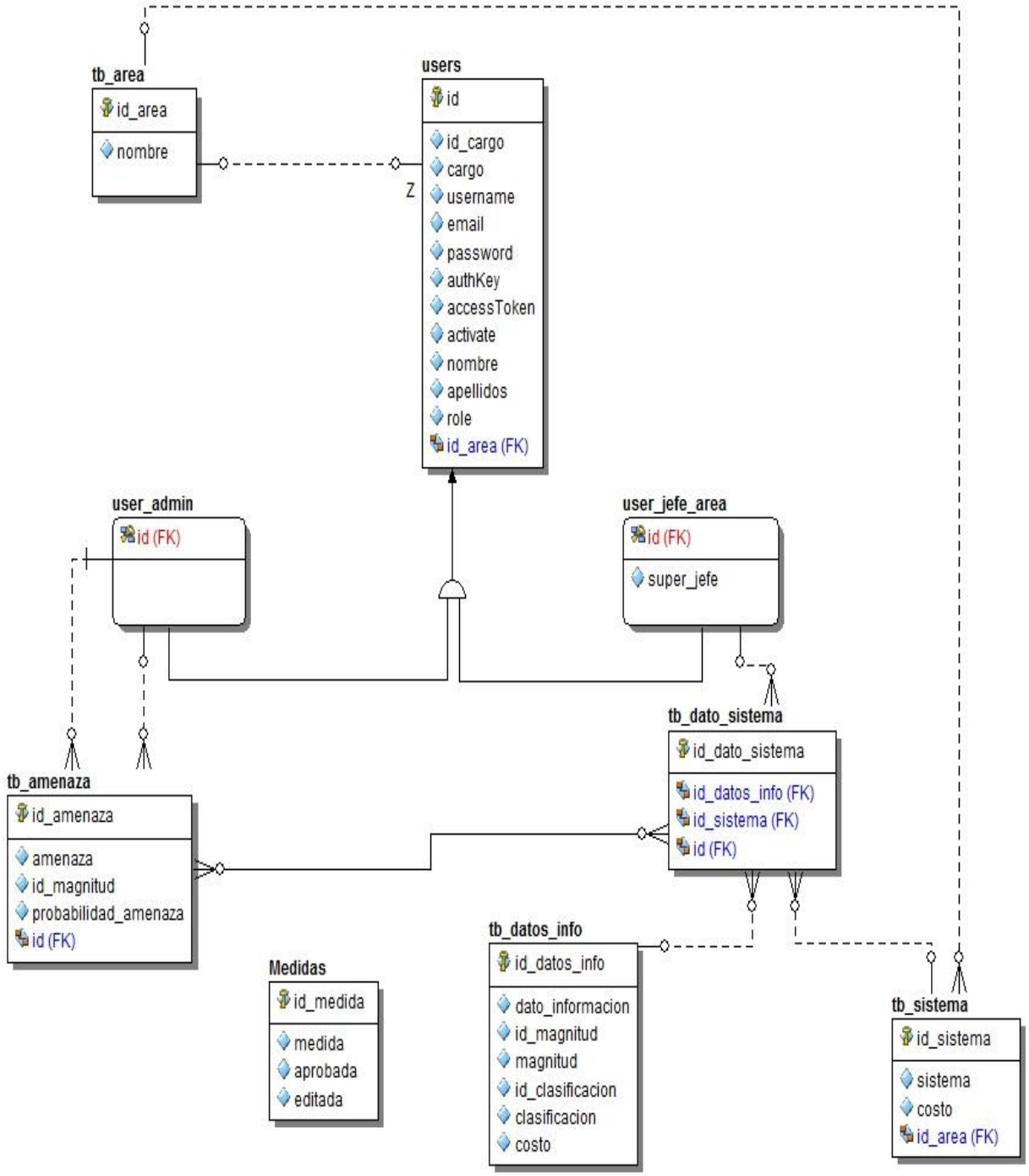


Anexo C15. Visualizar Matriz de Riesgos



Anexo D-Diseño de la BD

Anexo D1. Modelo lógico de datos



Anexo D2. Modelo físico de datos