UNIVERSIDAD DE SANCTI SPÍRITUS
José Martí Pérez

TyE

DEPARTAMENTO DE INGENIERÍA INFORMÁTICA

CARRERA: INGENIERÍA INFORMÁTICA

TRABAJO DE DIPLOMA PARA OPTAR POR EL TÍTULO DE

INGENIERO INFORMÁTICO

Sistema de Gestión de los incidentes y reportes de la seguridad informática en la Universidad de Sancti Spíritus "José Martí Pérez"

Mnagement and administration system for the incidents and reports of cybersecurity in the University of Sancti Spíritus "José Martí Pérez"

Autor: Somar Mahmoud

Tutor: Dr. C. Carlos Lázaro Jiménez Puerto
Ing. MSc. Julio Companioni Martínez

Sancti Spíritus, 2023

En enero del 2019 tomé la decisión de cambiar mi carrera de medicina a ingeniería informática, lo cual conllevaba un cambio del rumbo al futuro y un giro de 360 grados, de esa decisión he aprendido tres cosas fundamentales:

Primero, nunca es tarde para perseguir los sueños y las metas.

Segundo, no importan las sircunstancias y las situaciones siempre que se quiere llegar lejos se puede y siempre que se quiere brillar se puede.

Tercero, el apoyo de la familia y de los seres queridos en dichas situaciones es el pilar en el cual he podido sostenerme y construir el camino a mi futuro.

Con lo anterior dicho me gustaría dedicar mi tesis de grado a mi abuelo que en paz descanse, mi abuelo es uno de mis ídolos y me ha ensñado muchos valores que hoy en día sin esos valores no hubiera llegado tan lejos, mis padres queridos, a mi querida esposa y a toda mi familia en Cuba y Siria por todo el apoyo y el sacrificio que me han brindado en todo el viaje, por el hecho de estar a mi lado aunque algunos estén lejos en mis mejores y peores momentos, por todo el amor, cariño y dedicación que me han dado, por todas las lágrimas, sonrisas y valentía que me han compartido y sobre todo por nunca dudar en mí en ningun momento por lograr mis sueños.

AGRADECIMIENTOS

Dice el gran Economista y Filósofo Escocés Adam Smith que «la gratitud es la emoción que mueve al ser humano a recompensar a otro. La gratitud nos impele a darle al otro lo que hemos recibido.»

Me gustaría agradecer a las siguientes personas:

Mis padres y hermana por todo el al apoyo moral, económico y sacrificio que me han brindado a lo largo de la carrera.

Mi querida esposa por todo el amor, dedicación y cariño que me ha brindado desde el momento que la conocí, por aconsejarme y darme tranquilidad en todos mis momentos de frustración, por el gran corazón que tiene y por estar a mi lado celebrando los momentos más felices y darme ánimo, apoyo y amor en los momentos más difíciles.

Mi familia tanto en Cuba como en Siria por toda la tranquilidad que me han ofrcido.

Todos mis amigos y compañeros de clase por toda la ayuda y paciencia que han tenido conmigo especialmente a Royk Legón Ojito, Dairon Alejandro Ortíz Gelabert y a Jorge Luis Gonzalez Lage no solo por el apoyo emocional sino por los debates e intercambios en todos los espacios cuando más se les necesitaba.

Mis Profesores por formarme como ingeniero informático especialmente al profesor Arley Ulloa Zaila por su grandes esfuerzos en enseñar y formar al estudiante y a Julio Companioni Martínez por su paciencia y dedicación,a la profesora LLidia Rosa Ríos por su gran corazón y manera de atender especialmente en los momentos con más dudas y a la Dr. C. María de las Mercedes Calderón Mora por la gran guía y esfuerzo que me ha brindado en incluirme ne proyectos de alto impacto.

Mi tutor, mentor y guía el Dr. Carlos Lázaro Jiménez Puerto por su gran esfuerzo en sacar

el máximo provecho de mi a lo largo de toda la trayectoria, por su dedicación a todos mis problemas a lo largo del camino, por su infinita paciencia a la hora de ayudar, por enseñarme y guiarme en todos los aspectos tanto académicos como investigativos, por estar presente en todo momento y no dudar nunca en ayudarme y darme respuesta a todas mis inquietodes y dudas, por mostrarme el camino al éxito y formarme como futuro ingeniero informático.

A todos los que han participado de una manera u otra. GRACIAS de todo Corazón.

RESUMEN

La Seguridad informática es una de las disciplinas más importantes hoy día a nivel mundial, con el rápido crecimiento y avance de las tecnologías digitales se ha convertido en un tema de suma importancia en toda institusión. Cuba no está auesente de esta disciplina, aunque aún es incipiente. Específicamente en la Universidad de Sancti Spíritus «José Martí Pérez». El departamento y grupo de Seguridad Informática de la misma es el encargado de brindar los servicios de seguridad a la institusión y proteger la información de la Universidad, la manera en la que lo realizan es a través de una serie de reportes e informes que se procesan ante algún incidente recopilando datos e información relevantes al mismo con el fin de procesar dichos reportes. En la presente investigación se desarrolló un sistema de gestión para los incidentes de la seguridad informática para facilitar y agilizar la gestión de los reportes de incidentes de Seguridad Informática que se ajusten a las necesidades del cliente. Empleando para su desarrollo la metodología RUP y UML, como lenguaje de modelado, se seleccionó el lenguaje de programación Python haciendo el uso de su framework de desarrollo Django y el motor de base de datos PostgreSQL.

ABSTRACT

Cybersecurity is one of the most important disciplines worldwide today, with the rapid growth and advancement of digital technologies it has become an issue of utmost importance in every institution. Cuba is not absent from this discipline, although it is still incipient. Specifically at the University of Sancti Spíritus "José Martí Pérez". The IT Security department and group is in charge of providing security services to the institution and protecting the University's information assets. The way they proceed is through a series of reports. that are processed in the event of an incident, collecting data and information relevant to it in order to process said reports. In this research, a Cybersecurity incidents management system was developed to facilitate and streamline the management of Cybersecurity incident reports that adjust to the client's needs. Using RUP and UML methodology as a modeling language for its development, Python programming language was selected using its Django development framework and PostgreSQL database engine.

ÍNDICE

FIGURAS

TABLAS

INTRODUCCIÓN

Introducción:

En la década de los 1950 inició el desarrollo de las redes computacionales con el surgimiento de las primeras redes informáticas. En este momento que se enmarca el surgimiento del término seguridad informática, que durante la década de 1960 se redefinió con constructos teóricos más cercanos a los que hoy conocemos.

Teniendo en cuenta lo anterior, se puede separar esta disciplina en dos partes: antes y después de la invención del Internet. Antes del Internet, la única forma de dañar un disposi- tivo era acceder físicamente a él, por lo tanto, el delito era considerado como "allanamiento de morada" y no ciberataque. Después de la invención del Internet a finales de los 60 fue cuando nace el ciberespacio, lo que significó un nuevo entorno y una nueva posibilidad para los ciberdelincuentes.

El primer ciberataque que se conoce fue a través de internet en enero de 1996 y se realizó con técnicas muy parecidas a lo que hoy se conoce como phishing (pesca). Este fue lanzado contra la compañía America Online (AOL), una empresa de servicios de internet y medios con sede en Nueva York. Los atacantes utilizaron el correo electrónico o el método de mensajería de la compañía para conseguir que los usuarios de AOL divulgaran sus contraseñas.

A medida que las empresas comenzaron a utilizar la web, controlar el acceso a los datos en los sistemas se convirtió en un punto importante de preocupación. Entre las primeras medidas para proteger la información se incluye el procesamiento de periodos, donde se separaban las acti-

vidades por partes y los usuarios podían manipular la información en un tiempo determinado, establecido por los expertos de Seguridad Informática.

Es indudable que la seguridad de los sistemas informáticos de cualquier organización se ha convertido en uno de los pilares más sostenibles y vulnerables, y se hace imprescindible la búsqueda de los mecanismos para fortalecerla. El plan de la seguridad se convierte en una herramienta fundamental en el tratamiento de la información, en la explotación de los recursos tecnológicos y en el desarrollo de nuevas aplicaciones y tecnologías para la imple- mentación de sistemas más avanzados a escala internacional.

La proliferación de la nube, de los servicios remotos, de las aplicaciones contratadas como servicios, de dispositivos cada vez más vulnerables, del desarrollo tan rápido de los sistemas operativos, el uso de software con variadas funcionalidades y para múltiples usuarios tienen un impacto en la explotación de las tecnologías de la información y las comunicaciones (TIC) en la sociedad que abre un universo de inmensas estrategias maliciosas que pueden acabar con cualquier organización.

En la actualidad, la seguridad informática no es solo un tema importante para las grandes empresas, sino también para los individuos. Con la creciente cantidad de información personal almacenada en dispositivos digitales y la transmisión de información a través de redes, se ha convertido en un tema crítico para la protección de la privacidad y la integridad de los datos. Por esta razón, cada vez más personas toman medidas para proteger sus sistemas y datos de las amenazas cibernéticas.

Cuba no es la excepción, el avance de la seguridad informática se ha notado y ha cobrado auge en los últimos años a partir del proceso de informatización de la sociedad cubana, el surgimiento de la Universidad de Ciencias Informáticas (UCI) en 2003 y la apertura en esta de programas orientados a la seguridad informática (ciclo corto y carrera universitaria).

Indudablemente, los constantes cambios en los que ha estado inmersa la sociedad han tenido su reflejo en el Sistema de Educación Superior. Cuestión que impulsó el trabajo colaborativo, en redes académicas, científicas, sociales y la gestión de proyectos nacionales e internacionales **?**. El cumplimiento de esta tarea no resultaba factible desde los postulados de una enseñanza tradicional que centra la atención en el docente como transmisor de conocimientos y valores que son reproducidos por los estudiantes, por tanto, fue necesario mutar del modelo tradicional de educación a otro que responde a las demandas del siglo XXI.

En correspondencia dirección del país desarrolló una estrategia de adopción de las TIC en todo el sistema educacional, que integra la interconexión de centros atendidos por el Ministerio de Educación, a la Red de redes, teniendo como premisa su carácter integrador de las TIC. De esta manera se definieron lineamientos "orientados a perfeccionar el sistema de ciencia e innovación, con clara referencia a las universidades"**?**; instituciones que por excelencia son generadoras de nuevos conocimientos.

La Universidad de José Martí Pérez de Sancti Spíritus (UNISS) cuenta con un grupo de seguridad informática, subordinado al rector, para mantener el control y la seguridad de los datos personales y profesionales de todas las estructuras de la organización. Durante el desarrollo de las prácticas laborales y en el cumplimiento de las actividades propias de este grupo, se identificaron las siguientes problemáticas prácticas:

1. La gestión de la documentación que se realiza desde el grupo no está informatizada, lo que incurre en demoras y gastos de recursos.
2. No existe una base de datos donde se almacenen los informes de los incidentes ocurridos, cuestión que dificulta la obtención de información relativa a tipos de incidentes más frecuentes, segmentos de usuarios a los que están dirigidos y las tendencias por períodos.
3. Insuficiente cultura acerca de la naturaleza y consecuencias de los incidentes de seguridad informática.
4. La falta de cultura y conocimiento sobre la seguridad informática en toda la universidad.

Por tanto, el grupo se propone, a través de la información, gestión y planificación, brindar los servicios previstos en su misión para toda la estructura de la organización y expandir la cultura de los usuarios en esta rama de la informática.

Las demandas sociales actuales exigen de la universidad un proceso de gestión de la se- guridad informática consciente, basado en un proyecto flexible y competente, que prometa cobertura suficiente y satisfaga las necesidades de la organización, y resuelva las carencias y necesidades de sus profesionales, de ahí se deriva el siguiente problema de investigación: ¿Cómo contribuir al proceso de gestión de la seguridad informática en la Universidad de Sancti Spíritus "José Martí Pérez"? Se define como objeto de estudio el proceso de gestión de la seguridad informática.

De acuerdo con la problemática planteada se propone como objetivo de la investigación:

Desarrollar un sistema informático que contribuya al proceso de gestión de la seguridad informática de la Universidad de Sancti Spíritus “José Martí Pérez”.

Para dar solución al problema de investigación se formularon las siguientes preguntas de investigación:

1. ¿Cuáles son los fundamentos teóricos, metodológicos y tecnológicos que sustentan el desarrollo de un sistema informático para la gestión de la seguridad informática en la Universidad de Sancti Spíritus “José Martí Pérez”?
2. ¿Cómo desarrollar un sistema informático para la gestión de de la seguridad informática en la Universidad de Sancti Spíritus “José Martí Pérez”?
3. ¿Cómo validar el correcto funcionamiento de un sistema informático para la gestión de los incidentes de la seguridad informática en la Universidad de Sancti Spíritus “José Martí Pérez”?

En correspondencia con las preguntas de investigación se definieron las siguientes tareas de investigación:

1. Determinar los fundamentos teóricos, explicando los antecedentes bibliográficos, las bases teóricas y la definición de términos necesarios para comprender los cimientos del desarrollo de un sistema informático para la gestión de información.
2. Determinar los elementos metodológicos que contribuyan al desarrollo ágil, robusto y escalable de un software de gestión de información.
3. Determinar los fundamentos tecnológicos que permitan garantizar la usabilidad, se- guridad y calidad de la solución que se desea desarrollar.
4. Desarrollar un sistema informático utilizando la metodología seleccionada para facilitar la gestión de los datos asociados a la seguridad informática en la UNISS.
5. Validar el correcto funcionamiento del sistema informático para la gestión de los datos asociados a los incidentes de la seguridad informática en la UNISS.

La metodología empleada asume, como criterio fundamental, la concepción marxista leninista con un enfoque materialista dialéctico a partir de una concepción sistémica de la in- vestigación, dando lugar a una propuesta flexible como alternativa de solución, susceptible a comprobación científica; se emplearon los siguientes métodos de la investigación científica.

Del nivel teórico:

- Análisis histórico-lógico que permitirá estudiar el modo en que han evolucionado los estándares y normas para la gestión de la seguridad informática.
- Analítico-sintético el cual posibilitará hacer un estudio de los principales Sistemas de Gestión de seguridad informática, así como las tendencias en la gestión de incidentes y detec- ción de vulnerabilidades, para posteriormente sintetizar y aplicar el conocimiento adquirido, de modo que se logre un mayor entendimiento y se pueda arribar a conclusiones que con- tribuyan a la solución del problema planteado.
- Modelación: Se utilizará para lograr una mejor comprensión de los procesos asociados a la gestión de la seguridad informática, a partir de la representación en el modelo de dominio de entidades y actores.

Del nivel empírico:

- Observación, que guiará el estudio del estado del arte, permitiendo realizar un análisis sistémico, selectivo y objetivo de los principales sistemas que en la actualidad pueden realizar la gestión de la seguridad informática.
- Entrevista no estructurada con la intención de obtener información referente a los procesos de gestión de incidentes y detección de vulnerabilidades, así como criterios de expertos en el tema.

Con lo acordado anteriormente la visión del grupo de seguridad informática de la UNISS consiste en:

- El estudio de los escenarios existentes en materia de la inseguridad de la información. • Integración de nuevos elementos tecnológicos que permitan minimizar los riesgos, amenazas y vulnerabilidades en la red.
- Aplicación y mejoramiento de sistemas que permitan optimizar los procesos de tratamiento y/o protección de la Información.
- Asesoría e implementación de mecanismos de seguridad y protección en sistemas informáticos.

El informe de la tesis se estructuró de tesis queda estructurado en tres capítulos, arribándose a conclu- siones concretas, seguido de las recomendaciones correspondientes y referencias

bibliográficas.

En el Capítulo 1 se recoge el marco teórico referencial y los principales conceptos que constituyen la base teórica de la investigación, abordando temas Como la seguridad infor- mática, los incidentes de seguridad informática, los diferentes tipos de reportes de cada in- cidente, las categorías y subcategorías de ataques cibernéticos y el proceso de gestión infor- mático. También en el primer capítulo se analizan las principales tendencias tecnológicas con el objetivo de seleccionar las adecuadas para el desarrollo del sistema informático requerido.

En el Capítulo 2 se caracteriza el obje- to de estudio y se describe el desarrollo del software a través de la metodología seleccionada, desarrollando la modelación del negocio, definiendo las necesidades y cualidades del sistema, y mostrando el diagrama entidad-relación así como el modelo físico de la base de datos.

En el Capítulo 3 se realiza la validación de la solución propuesta a través de pruebas de aceptación de software mostrando las principales interfaces y funcionalidades del prototipo inicial. Para finalizar, un apartado de conclusiones 3.5 donde se verifica el cumplimiento de los objetivos tra- zados al inicio de la investigación, así como recomendaciones 3.5, donde se plasman una serie de propuestas encaminadas a la continuidad de esta investigación.

CAPÍTULO 1

Fundamentos teóricos, metodológicos y tecnológicos que sustentan la implementación de un sistema informático para la gestión de los incidentes asociados a la seguridad informática en la Sancti Spíritus «José Martí Pérez»

Este capítulo recogeo se recoge el marco teórico referencial y los principales conceptos que con- stituyen la base teórica de la investigación, abordando temas Como la seguridad informática, los incidentes de seguridad informática, los diferentes tipos de reportes de cada incidente, las categorías y subcategorías de ataques cibernéticos y el proceso de gestión informático. También en el primer capítulo se analizan las principales tendencias tecnológicas con el objetivo de seleccionar las adecuadas para el desarrollo del sistema informático requerido.

1.1. Gestión de incidentes de seguridad informática

1.1.1. La Gestión

En términos generales, la gestión es una serie de tareas que se realizan para acometer un fin planteado con antelación**?**.

La gestión como objeto de estudio ha sido abordada por autores como Deming, quien desarrolló conceptos acerca de que la generación de productos y servicios que obtuvieran la satisfacción del cliente, se traducía no solo en los esfuerzos de la mano de obra, sino también en el análisis y mejoramiento de las etapas de la producción, como la sistematización del ciclo Deming/Schewhart que reconoce como etapas: planificar, hacer, verificar y actuar**?**.

la gestión ya sea empresarial o de cualquier otro tipo de la información es uno de los asuntos más importantes de toda institución, empresa organización. . . etc. La razón de su im- portancia es la facilidad de la administración en el lugar de trabajo y el manejo del trabajo.

Conseguir una organización acertada es una de los objetivos de la gestión, y su principal función debe ser la de evitar solapar esfuerzos y responsabilidades. Para ello, se deben establecer relaciones efectivas de autoridad y responsabilidad,. La gestión se encarga de colocar en cada vacante al trabajador adecuado, con las habilidades, cualificación y entrenamiento adecuados.

1.1.2. Seguridad Informática

La sociedad de la información, la ausencia de fronteras y la inmaterialidad de la comu- nicación a través de las Tecnologías de la Comunicación y la Información, conducen en el ámbito del Derecho Penal, a la escasa relevancia de los límites temporales y espaciales que han constituido, tradicionalmente, su límite. La delincuencia informática y los delitos rela- cionados con ella, suponen un tipo de criminalidad característica y especial; y con la expre- sión delito informático, cibercrimen o ciberdelito se define a todo ilícito penal llevado a cabo a través de medios informáticos, incluido el blanqueo de capitales**?**.

Hoy en día hay infinidad de métodos para violar la seguridad de un sistema o de una persona. En el mundo de alta tecnología actual, las creencias, opiniones y actitudes se moldean a medida que las personas interactúan con otras en las redes sociales y a través de Internet. Las

historias de fuentes noticiosas acreditadas y los hallazgos científicos son cuestionados por actores que participan activamente en operaciones de influencia en Internet. Los lobos solitarios y las grandes máquinas de propaganda perturban el discurso civil, siembran discordia y difunden desinformación. Bots, cyborgs, trolls, títeres de calcetines, deep fakes y memes son sólo algunas de las tecnologías utilizadas en la ingeniería social destinadas a socavar la sociedad civil y apoyar agendas adversas o comercialesCarley (2020).

Entendemos de la ciberseguridad como la protección de activos de información, mediante el tratamiento de las amenazas. Con el uso de las Tecnologías de la Información y la Comunicación, se facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, que conlleva serios riesgos y amenazas en un mundo globalizado; y las amenazas en el espacio digital adquieren una dimensión global que va más allá de la tecnología**?**.

En la gran mayoría de las organizaciones empresas e instituciones se manejan distintas maneras para la gestión de la seguridad de la información. Una de las maneras más populares y usadas es a través de los reportes de los incidentes que ocurren en las mismas.

Según ISOTools Excellece la seguridad informática, con sus siglas en inglés IT security, es la disciplina que se encarga de llevar a cabo las soluciones técnicas de protección de la información. "La seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, podríamos decir, que se trata de implementar medidas técnicas que preservarán las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa"**?**.

1.1.3. Incidentes

Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella**?**.

Hay muchas maneras de poder identificar un incidente de seguridad, entre ellas, las prin- cipales son:

- Monitorizar adecuadamente los sistemas, al menos los críticos para el negocio o que con- tienen información sensible o confidencial.
- Implantar herramientas de correlación y revisión de logs de los principales sistemas para detectar posibles incidentes de seguridad o patrones de comportamiento anómalos.
- Implementar un servicio de ciberinteligencia que pueda detectar fugas de datos, contraseñas comprometidas...etc.
- Concienciar a los usuarios en la importancia de comunicar cualquier incidente de seguridad que hayan sufrido o que crean haber sufrido, o cualquier comportamiento extraño que detecten.

El eslabón más débil en cuanto nos referimos a incidentes de seguridad siempre es el propio personal de las organizaciones, que bien accidentalmente o de manera intencionada pueden ocasionar o ser colaboradores necesarios para que se produzca un incidente de estas características**?**.

1.2. Gestión en la seguridad informática

1.2.1. Importancia

La toma de decisiones en la gestión de incidencias es de vital importancia en la ejecución de las funciones de los directivos en las organizaciones, ya que provee a la máxima dirección de las empresas e instituciones que permite analizar, discutir e interpretar los resultados de las incidencias**?**.

El éxito de una organización está enmarcado en las decisiones que gestione su personal, esto amerita que la gerencia tome las decisiones correctas en cuanto a su desempeño y ejecución. Para ello la organización debe emplear día a día nuevas estrategias con el propósito de crear ventajas competitivas. En este contexto la tecnología se ha convertido en una de las herramientas básicas de la organización, ya que forma parte de la cotidianidad del ser humano y de la sociedad. El individuo es capaz de pensar, organizar y tomar decisiones a nivel personal y laboral, consciente de que existe un constante avance tecnológico que contribuye en la toma

de decisiones, en cuanto a lo que es más conveniente tanto para los trabajadores como para la organizaciónAlvarado et al. (2018).

La gestión de los incidentes en la seguridad informática es de vital importancia para toda institución, ya que una buena gestión viene acompañada de una gran organización lo cual facilita el trabajo y evita la pérdida de recursos.

1.2.2. Evolución Histórica

La gestión como se ha mencionado antes es el arma necesaria para la organización y administración de toda institución. La gestión ha ido evolucionando a lo largo de la historia con el desarrollo de la tecnología, desde un principio se intentaba gestionar el trabajo de una institución usando el formato duro o el papel donde se realizaban reportes e informes en un papel para así guardarlo. A medida de que la tecnología fue avanzando el campo de la gestión ha tomado un giro grande, se fue remplazando el formato duro por el formato digital.

En la seguridad informática las formas y maneras de gestionar los reportes, infomres e incidentes han ido cambiando a medida de que ha ido desarrollando la tecnología. En un primer momento los reportes de incidentes en las instituciones se procesaban en planillas de Word o Excel donde se recogían todos los datos del incidente y se rellenaban las planillas con dichos datos, luego se procedía a imprimir los documentos y se archivaban en formato duro. A medida que ha ido avanzando la tecnología empezaron los cambios en el procesamiento y la gestión de los reportes e informes, actualmente las instituciones cuentan con sistemas de gestión donde se procesan todos los incidentes y se pueden guardar en una base de datos para un futuro uso de los mismos y así tener una mayor protección de los datos y evitar su destrucción.

1.2.3. Normas

Al vivir en una era dependiente de la tecnología, y con el rápido crecimiento de las herramientas informáticas, la seguridad no solo se debe encontrar en los sistemas informáticos sino tambien en normas gubernamentales para así tener precauciones con aquellas personas que intentan vulnerar algún sistema o persona.

En Cuba existen varias leyes sobre la seguridad informatíca, una de ellas se encuentra en la

resolución 105 del decreto de ley 360 Sobre la Seguridad de las Tecnologías de la Información y la Comunicación para la informatización de la sociedad y la Defensa del Ciberespacio Nacional de (31 de mayo del 2019 en su Artículo 25 inciso d), regula que el Ministerio de Comunicaciones en coordinación con los ministerios del Interior y de las Fuerzas Armadas Revolucionarias, establece el Modelo de Actuación Nacional para la respuesta a incidentes de Ciberseguridad y asegura los procedimientos para su implementación en todos los niveles por parte de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, así como realiza el enfrentamiento y neutralización de estos sucesos de acuerdo a lo que a cada organismo le corresponde.

También algunas acciones se concretaron en el Decreto-Ley No. 370/2018 "Sobre la informatización de la Sociedad en Cuba" del Ministerio de Justicia [MINJUS], entendido como: El proceso de aplicación ordenada y masiva de las Tecnologías de la Información y la Comunicación en la gestión de la información y el conocimiento, con la seguridad requerida, para satisfacer gradualmente las necesidades de todas las esferas de la vida social, en el esfuerzo por parte del Estado de lograr cada vez más eficacia y eficiencia en los procesos, así como mayor generación de riquezas y aumento de la calidad de vida de los ciudadanos.

1.2.4. Sistemas de Gestión de Incidentes de Seguridad Informática encontrados

La seguridad de la información es un tema necesario en toda organización por lo cuál algunas de ellas han implementado sus propios sistemas de gestion de la seguridad. Después de una busqueda de dchos sistemas sehan encontrado los siguientes que contienen algunas semejanzas al sistema desarrollado en este proyecto:

- Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para el departamento de tecnlologías de la información y comunicación del distrito 18D01 de educación**?**.
- Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín**?**.

Los sistemas mencionados anteriormente contienen herramientas para la gestión de los incidentes de la seguridad informática en distintas áreas y con diferentes normas de acuerdo a las

normas establecidas por el país de procedencia y la institución a la que pertenencen.

1.3. Metodologías y Herramientas

El desarrollo de software no es una tarea fácil. Prueba de ello es que existen numerosas propuestas metodológicas que inciden en distintas dimensiones del proceso de desarrollo. Por una parte se encuentran aquellas propuestas más tradicionales que se centran especialmente en el control del proceso, estableciendo rigurosamente las actividades involucradas, los artefactos que se deben producir, y las herramientas y notaciones que se deben usar**?**.

1.3.1. Metodologías del desarrollo

En la actualidad la rapidez y el dinamismo en la industria del software han hecho replantear los cimientos sobre los que se sustenta el desarrollo de software tradicional**?**.

Existen una gran variedad de metodologías de desarrollo de software, con diferencias significativas en cuanto al tipo de proceso empleado y productos obtenidos, cantidad de recursos involucrados, tiempos de desarrollo y estructura organizacional requerida**?**.

Entre las metodologías más conocidas y usadas a nivel mundial existen las metodologías de desarrollo ágil entre ellas se encuentra:

- XP (Extreme Programming): La programación extrema es una metodología ágil de gestión de proyectos que se centra en la velocidad y la simplicidad con ciclos de desarrollo cortos y con menos documentación. La estructura del proceso está determinada por 5 valores fundamentales, 5 reglas y 12 prácticas de XPAsana (2022).
- SCRUM: La metodología Scrum es un proceso para llevar a cabo un conjunto de tareas de forma regular con el objetivo principal de trabajar de manera colaborativaapd (2020).

A pesar de que las metodologías ágiles como el nombre lo indica son maneras y formas muy ágiles para el desarrollo de software, se encuentra otra metodología para el desarrollo llamada RUP o por sus siglas en inglés «Rational Unified Process» (Proceso de Unificado Racional). Dicha metodología es conciderada como una de las mejores metodologías del desarrollo debido a su alta y extensa documentación para el desarrollo del software.

RUP es una metodología híbrida para el desarrollo de software que combina las mejores prácticas de los métodos ágiles y tradicionales (Scrum y RUP), con el objetivo de unir esas fortalezas y disminuir las debilidades para satisfacer al cliente en su totalidad y mantener un producto de calidad**?**.

En este trabajo se utilizará la metodología RUP como principal metodología del desarrollo del software.

1.3.2. Lenguajes de programación

Cutting y Stephen plantean que debe elegir el lenguaje de programación según los obje- tivos planteados. En el caso de que se quiera hacer un juego, un lenguaje como JavaScript, Java, C o C ++ podría funcionar, y si se espera realizar un buen trabajo con la Web, o Inteligencia Artificial, etc., lenguajes como Python, JavaScript o Ruby son buenas opciones. De esta manera, desde el inicio se debe saber que tipo de sistema informático se quiere desarrollar, o elegir un área de interés. A partir de ahí según sus inclinaciones, se debe elegir el lenguaje**?**.

Para esta investigación se usaron los siguientes lenguajes de programación como lenguajes base del software:

- JavaScript: JavaScript fue creado por los pioneros de Internet, Netscape, en la década de los noventa para su uso con la entonces nueva tecnología de los navegadores. El lenguaje sigue vivo en Internet, proporcionando una funcionalidad y facilidad de uso adicionales para una miríada de sitios web.
- Python: Python fue lanzado en 1991, y se ha hecho bastante popular en los últimos años. Es un lenguaje de programación que permite trabajar con rapidez e integrar sistemas con mayor eficacia.

1.3.3. Sistemas gestores de bases de datos

Una base de datos es un conjunto formado por varias Tablas con alguna afinidad temáticaArias (2017).

Se define una base de datos como un conjunto de datos organizados y relacionados entre sí**?**.

Para éste proyecto se utilizó el gestor de base de datos PostgreSQL el cuál es: PostgreSql es un sistema de gestión de base de datos objeto-relacional, distribuido bajo licencia BSD y con su código fuente disponible libremente. Es el sistema de gestión de base de datos de código abierto más potente del mercado**?**.

1.3.4. Frameworks

Aunque se utilicen muchas tecnologías diferentes, los frameworks siguen siendo un aspecto esen- cial del proceso de desarrollo de sistemas conectados de forma inteligente. Dado que este sector aún está en sus inicios, actualmente no hay un claro vencedor en este campo**?**.

Para este proyecto se utilizaron los siguientes Frameworks:

Django: es un marco de trabajo (framework) para el desarrollo de aplicaciones web usando Pyt- hon. Considera algunas funcionalidades listas para usar que facilitan el desarrollo de aplicaciones web. Como resultado, no es necesario escribir todo el código ni usar tiempo para buscar errores de código en el framework**?**.

Django se basa en el estilo Modelo-Vista-Plantilla, y proporciona una división entre las reglas de negocio, los datos y la interfazC. G. y Devl (2021).

Bootstrap: Bootstrap es un framework front-end gratuito, cuyo objetivo es hacer que el desarrollo web sea más rápido y sencillo. También incluye plantillas de diseño basadas en HTML y CSS para formularios, tipografía, botones, navegación, tablas, modales, carruseles de imágenes y muchos otros componentes junto con otros complementos de JavaScript opcionales.

CAPÍTULO 2

Análisis y diseño de un sistema informático para la gestión de los incidentes de la seguridad informática en la Universidad de Sancti Spíritus «José Martí Pérez»

En este capítulo se trabaja con los conceptos referentes a la metodología de desarrollo de software seleccionada, Rational Unified Process (RUP), así como las herramientas y tecnologías aplicadas para la construcción del producto a desarrollar.

El proceso unificado racional (RUP), conocido simplemente como "proceso unificado", es un marco popular de desarrollo de software iterativo e incremental.**?**. también se define como un meta- proceso que permite configurar procesos iterativos e incrementales y se estructura en dos dimensiones: fases y disciplinas **?**.

Se realiza un estudio del modelo del negocio identificando las reglas, actores y trabajadores que intervienen en el negocio, así como el diagrama de caso de uso del negocio, diagrama de actividades y el modelo de objetos. Además, se presentan las necesidades y cualidades del sistema, mostrando los requerimientos funcionales y no funcionales, el modelo de casos de

uso del sistema, su descripción y los actores del mismo. Finalmente se muestran los diagramas correspondientes a las clases del diseño como también los relacionados a la base de datos.

2.1. Modelación del negocio

Un proceso de desarrollo de software es el conjunto de actividades necesarias para transformar los requerimientos del usuario en un sistema informático. Un proceso define quién está haciendo qué, cuándo y cómo alcanzar un determinado objetivo. El modelado del negocio es una técnica para comprender los procesos del negocio de la organización que ayuda al equipo de desarrollo a comprender los elementos que intervienen en los proceso de negocios y las necesidades actuales de los usuarios en las empresas, también ayuda tanto a entender la dinámica de la organización como los problemas actuales e identificar mejoras potenciales.

Un caso de uso del negocio presenta lo que el Negocio ofrece a los actores. El Negocio decidirá cómo realizarlos, bien sea manualmente, o bien sea automatizarlos parcial o totalmente **?**.

2.1.1. Identificación de los procesos del negocio

El modelo del negocio describe el negocio en términos de casos de usos del negocio, que corresponde a lo que generalmente se le llama procesos **?**.

La identificación de los procesos del negocio consiste en identificar entidades y trabajadores que participan en la realización de los casos de uso del negocio **?**.

A partir de lo anterior se identifica el siguiente proceso de negocio:

- Gestión de los incidentes y reportes de la seguridad informática.

El procedimiento para realizar un reporte de un incidente comienza cuando ocurre una violación a las normas establecidas de la seguridad informática en la universidad o cuando ocurre un ataque a los servidores de la universidad donde se realizan distintos reportes dependiendo de la situación. A continuación, se agrupa toda la información requerida por el especialista del grupo de seguridad informática en la universidad, el cual procesa el reporte en correspondencia al tipo de incidente en formato Word. Luego se entrega al Rector para aprobar la decisión tomada por el especialista.

- Gestión de los informes de visita a un área determinada de la universidad.

El procedimiento para realizar una visita/auditoría a un área específica de la univrsidad ocurre cuando el jefe del grupo de seguridad informática decide realizar una visita a un área para una revisión de los requisitos establecidos por el mismo. A continuación, se procede a hacer la visita y se recopila y agrupa toda la información necesaria del área a la cúal se le realizó la visita por el especialista, el cual revisa los requisitos y normas de seguridad establecidas y realiza el informe de visita en formato Word. Luego se entrega al jefe de área para su firma en el informe.

2.1.2. Reglas del negocio

Las reglas del negocio representan una serie de restricciones de la organización para realizar las actividades o asociadas a la información. Las mismas determinan las políticas y estructura de la información, regulan el funcionamiento de la empresa, describen restricciones y comportamientos, y aunque no son requisitos que influyen en ellos **?**.

A continuación, se exponen las que fueron identificadas:

- Los reportes de incidentes se realizan cuando ocurre un incidente en la Universidad.
- Las visitas/auditorías a las áreas se realizan por desición del jefe del grupo de seguridad informática, sin aviso previo al jefe de área.

Tabla 2.1: Actores del negocio

Actor	Descripción
Rector	Es quien se encarga de aprobar los reportes de los incidentes.
Jefe de área	Es el encargado de firmar el informe de visita correspondiente a su área.

Tabla 2.2: Trabajadores del negocio

Trabajador	Descripción
Especialista	Es el responsable en realizar los reportes de incidentes, las visitas e informes de visita a las áreas.

2.1.3. Actores y trabajadores del negocio

Un actor del negocio es cualquier individuo, grupo, entidad, organización, máquina o sistema de información externos; con los que el negocio interactúa. Lo que se modela como actor es el rol que se juega cuando se interactúa con el negocio para beneficiarse de sus resultados **?**.

A continuación, se presentan los actores, caso de uso del negocio y diagrama de actividad perte- neciente al caso de uso del negocio.

La 2.1 muestra el actor de negocio y su descripción, del proceso gestión de incidentes de reportes de sistema de gestión de los incidetnes de la seguridad informática en la Universidad..

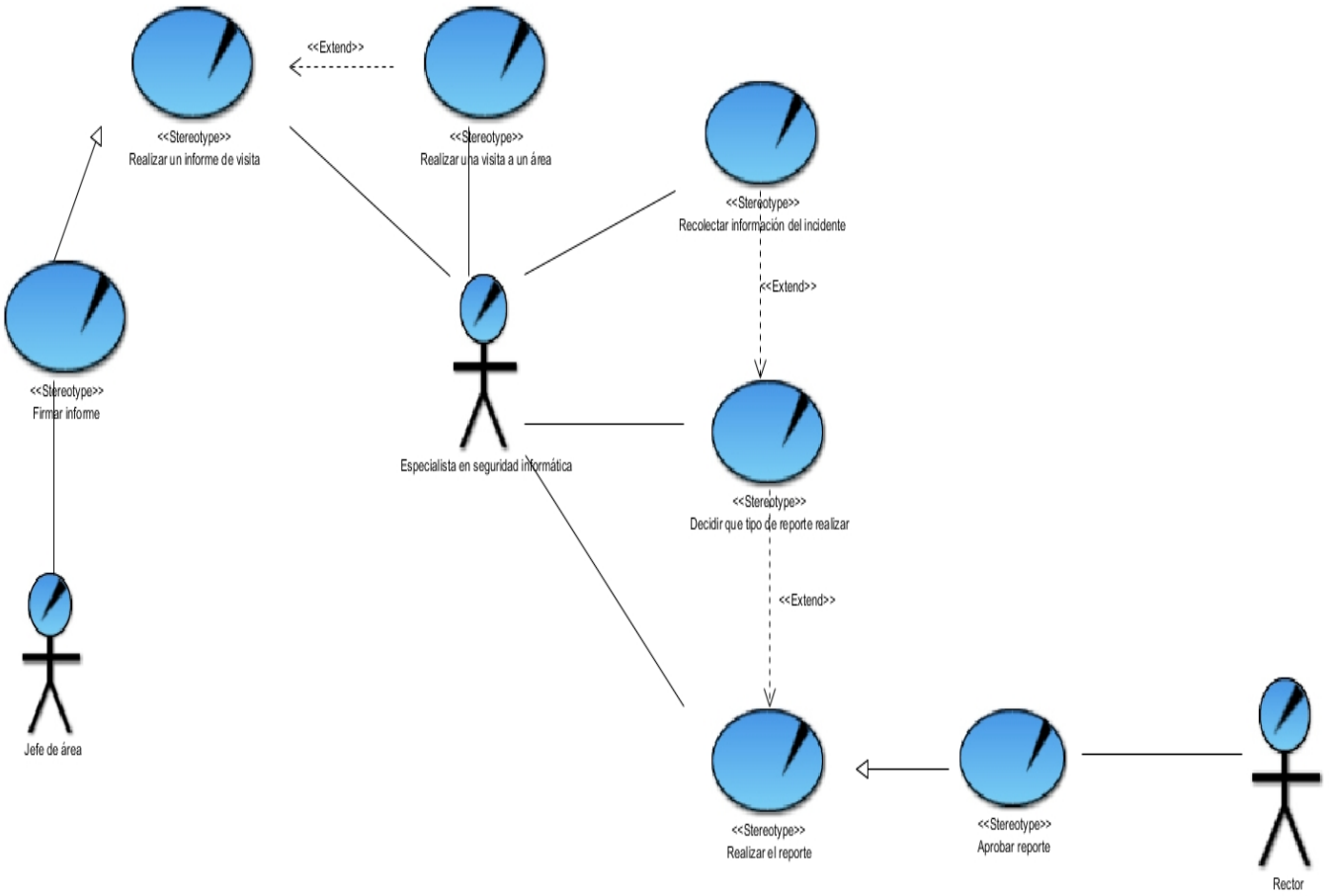
Los trabajadores del negocio son el punto de partida para derivar un primer conjunto de actores y casos de uso del sistem **?**. Un trabajador del negocio no es un actor del negocio. Es un representante del negocio con el cual un actor del negocio interactúa y que se transformará en un actor en los casos de uso del sistema, donde utiliza el sistema como herramienta para prestarle un servicio a los actores del negocio **?**.

En la Tabla 2.2 se muestran los trabajadores identificados en el negocio.

2.1.4. Diagramas de Casos de Uso del Negocio

El modelo de casos de uso del negocio describe los procesos de un negocio (casos de uso del negocio) y su interacción con elementos externos (actores), tales como los socios y clientes, es decir, su objetivo básico es describir las funciones que el negocio pretende realizar y como es utilizado por sus clientes y socios. Implica la determinación de los actores y casos de uso del negocio. Con esta actividad se pretende: Identificar los procesos en el negocio, definir las

Figura 2.1: Caso de uso del negocio informe de visita



fronteras que van a modelarse, identificando quién y qué interactuará con el negocio y crear diagramas del modelo de casos de uso del negocio **?**.

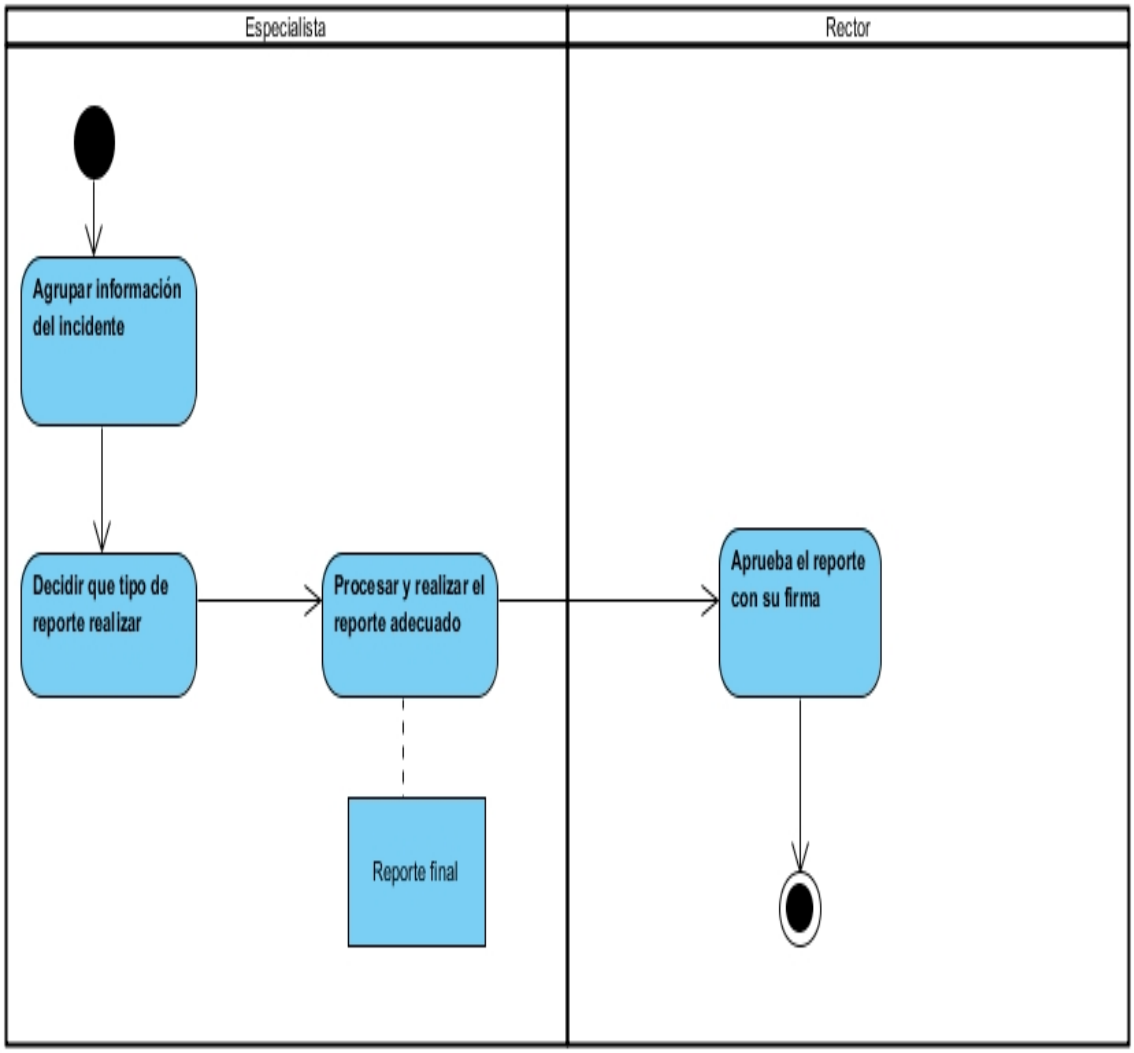
En la Figura 2.1 se muestra el trabajador del negocio que es quien inicia y se beneficia del caso de uso del negocio y el actor.

2.1.5. Diagramas de Actividad de los Casos de Uso del Negocio

El modelo de casos de uso del negocio describe los proceso de negocio de una empresa en términos de casos de uso del negocio y actores del negocio que corresponden con los procesos del negocio y con los clientes. Un modelo de casos de uso presenta un sistema (el negocio) desde la perspectiva de su uso y esquematiza cómo proporciona valor a sus usuarios. Se describe mediante diagramas de casos de uso **?**.

En la 2.2 se representa el diagrama de actividades para el caso de uso «Realizar reporte de incidente» correspondiente al proceso de gestión de incidentes de reportes de seguridad informática.

Figura 2.2: Diagrama de actividades caso de uso <<Realizar reporte de incidente>>



2.1.6. Modelo de Objetos

El diagrama de clases, como artefacto que se construye para describir el modelo de objetos del negocio, muestra la participación de los trabajadores y entidades del negocio y la relación entre ellos.

A continuación en la 2.3 e muestra el diagrama de clases del modelo de objetos para el caso de uso seleccionado.

2.2. Necesidades y cualidades del sistema

Las necesidades y cualidades del sistema establecen qué tiene que hacer exactamente el sistema que construyamos. Son el contrato que se debe cumplir, de modo que los usuarios finales tienen que comprender y aceptar los requisitos que se especifiquen. Los establecen los usuarios finales y participantes en los procesos.**?**.

Para poder identificar correctamente cuáles son los requerimientos de un proyecto, es necesario conocer las características del negocio en el que se inserta, es decir, los requisitos para la aplicación pueden ser derivados a partir del modelo de negocio **?**.

2.2.1. Requerimientos funcionales

Los requerimientos funcionales representan la funcionalidad el sistema, y se modelan mediante casos de uso **?**.

2.2.2. Requerimientos no funcionales

Los requerimientos no funcionales son los atributos que debe exhibir el sistema como facilidad de uso, fiabilidad, eficiencia, portabilidad, etc **?**.

Apariencia o interfaz externa

- La interfaz estará 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. Se cuidará porque la aplicación sea lo más interactiva posible.

Usabilidad

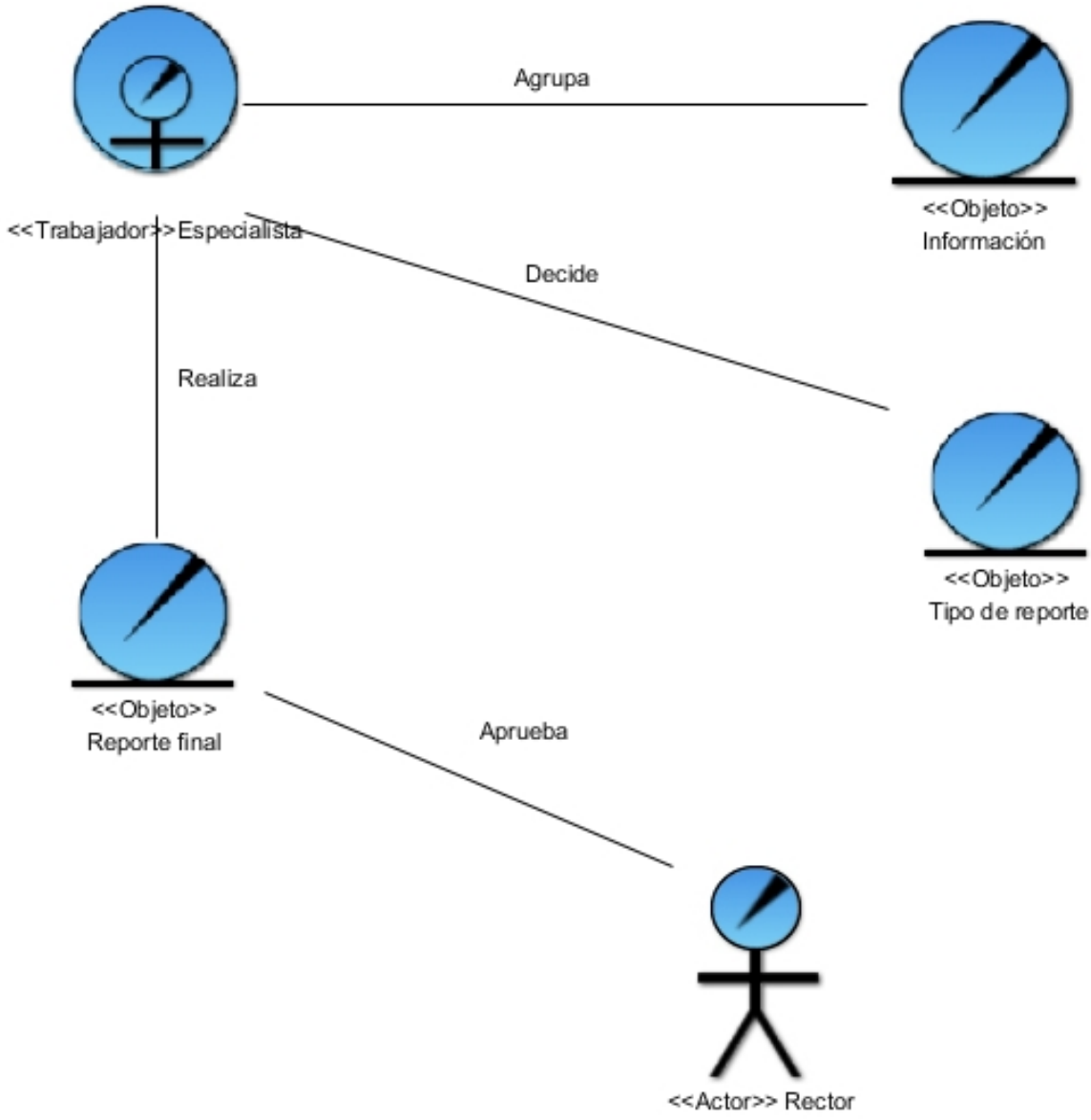
- La aplicación web podrá ser usada por aquellos usuarios que no tengan experiencia en el uso de la computadora, sólo necesitarían un ligero entrenamiento sobre el funcionamiento de los principales elementos de una interfaz estándar en el ambiente de los Sistemas Operativos Windows y Linux (uso del mouse, manejo de menús, botones, cuadros de texto, entre otros).

Rendimiento

Tabla 2.3: Requisitos funcionales

Nº	**Requerimientos**
R 1	Autenticar usuarios
R 2	Gestionar usuarios
R 3	Gestionar trabajadores
R 4	Gestionar entidades afectadas
R 5	Gestionar áreas
R 6	Gestionar países
R 7	Gestionar provincias
R 8	Gestionar municipios
R 9	Gestionar categorías
R 10	Gestionar subcategorías
R 11	Gestionar Reportes CUCERT
R 12	Gestionar Reportes incidente/violación
R 13	Gestionar informes de visita
R 14	Planificar una visita
R 15	Ver visitas planificadas
R 16	Escanear una URL
R 17	Visualizar noticias de ciberseguridad

Figura 2.3: Diagrama de clases del modelo de objetos



- No se requiere de una capacidad de procesamiento alta sino mediana, pues la aplicación no ejecutará algoritmos complejos, sino medianamente complejos.

Soporte

- Se requiere un servidor de bases de datos con soporte de volúmenes medianos de información. Se documentará la aplicación para garantizar su soporte. Se realizará mantenimiento a fin de aumentar las funcionalidades del mismo a través de versiones posteriores y según las nuevas necesidades de los clientes.

Portabilidad

- El producto podrá ser utilizado sobre plataforma Windows, Linux u otro sistema operativo. La estandarización del protocolo de TCP/IP y HTTP permite la interacción del lado del cliente para los sistemas operativos más difundidos como los Sistemas GNU/Linux (Debian, Ubuntu, Nova, etc.), Windows o MacOS.

Seguridad

- Debe garantizar la conectividad e integridad de los datos almacenados a través de la red usando el protocolo de comunicación HTTPS y el SGBD respectivamente. Debe garantizar la confidencialidad para proteger la información de acceso no autorizado. Esto esta- rá garantizado por el Sistema Gestor de Base de Datos. El sistema impondrá un estricto control de acceso que permitirá a cada usuario tener disponible solamente las opciones relacionadas con su actividad. La información deberá estar disponible a los usuarios en todo momento, limitada solamente por las restricciones que estos tengan de acuerdo con la política de seguridad del sistema.

Integridad

- La información manejada está protegida contra la corrupción y los estados inconsistentes pues los mecanismos de validación y el administrador del sistema se encargarán de que los datos entrados sean confiables, de calidad y salvado para los casos de errores.

Disponibilidad

- Los usuarios tienen garantizado el acceso a la información sin ningún inconveniente y al mismo tiempo.

Requisitos legales

- La herramienta propuesta responderá a los intereses de la Universidad de Sancti Spíritus «José Martí Pérez» en correspondencia con la base normativa del manejo de los reportes de incidentes de seguridad informática aprobados el ministerio de informática y comunicación y los controles de la Oficina de Seguridad de las Redes Informáticas (ORSI) en Cuba.

Confiabilidad

- La aplicación en caso de fallos garantiza que las pérdidas de información sean mínimas y los datos almacenados no se pierden ni se modifiquen ya que los mismos solo son modificados cuando se confirma la acción requerida.

Software

- Del lado del cliente se espera un sistema que funcione en un navegador que interprete las funciones básicas de JavaScript, css3 y html5, como, por ejemplo, Google Chrome y Firefox.

Hardware

- Las computadoras situadas en los puestos de trabajo de los usuarios requerirán como mínimo un procesador Pentium IV, 512 Mb de memoria RAM. Estas máquinas deben estar conectadas en red con el servidor.
- Como servidor se requerirá un computador con un procesador Pentium IV, 2 Gb de memoria RAM y al menos 100 Gb de disco duro y sistema opertivo Linux preferiblemente de las versiones (Debian, Ubuntu).

2.2.3. Modelo de Casos de Uso del Sistema

El modelo de casos de uso describe las interacciones entre los actores y el sistema, y la meta de los actores al usar el sistema caso de uso. Para identificar los casos de uso del sistema se utiliza la tabla de eventos y generalmente la correspondencia no es uno a uno **?**.

Para definir los actores se analizaron todos los usuarios que tienen la responsabilidad de realizar alguna acción en el sistema, los mismos se muestran en la 2.4

Un diagrama de casos de uso del sistema describe lo que debe hacer el sistema para automatizar

Tabla 2.4: Actores del sistema

Actores del sistema	Descripción
Especialista en seguridad informática	Encargado de gesionar todos los datos de los reportes de incidetens, los informes de visita y la gestión de los usuarios del sistema.

uno o más pasos de la realización del caso de uso de negocio. Se representan los casos de uso del sistema, sus actores y las relaciones entre los casos de uso y sus actore **?**.

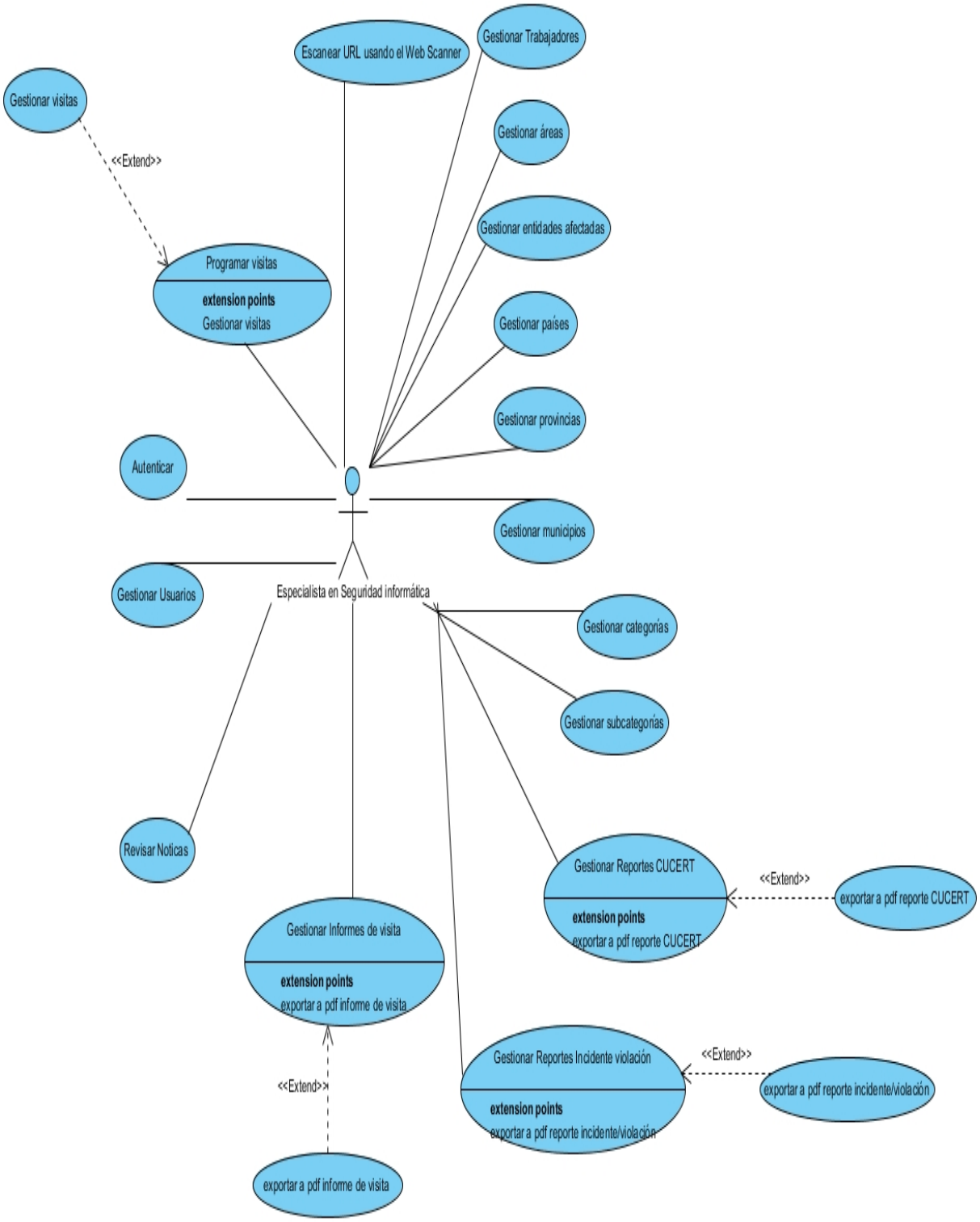
La 2.4 muestra los casos de usos del sistema que son importante para la arquitectura del mismo.

Para una mejor comprensión de los requerimientos solicitados por el usuario, se describen en la 2.5 el caso de uso más importante de la solución propuesta como parte de esta investigación: Gestionar Reportes CUCERT.

Tabla 2.5: Descripción de los casos de uso del sistema

Nombre del caso de uso	**Gestionar reportes CUCERT**
Actores	Especialista
Propósito	Visualizar todos o un reporte específico los reportes actuales, añadir y eliminar carreras, así como actualizar los datos de los ya insertadas en caso que sea necesario, también exportar alguno a formato pdf de ser necesario.
Resumen	El caso de uso incia cuando el especialista accede al apartado de los reportes CUCERT. Una vez dentro podrá visualizar todos o un reporte en específico, insertar un reporte nuevo, modificar o eliminar un reporte en caso de ser necesario.
Referencias	R11, R11.1, R11.2, R11.3, R11.4, R11.5
Precondiciones	Debe existir un informante, una entidad afectada, una categoría y una subcategoría insertados anteriormente
Acción del actor	**Respuesta del sistema**
1. El especialista desea adicionar, modificar, eliminar o exportar un reporte a formato pdf.	2. El sistema ejecuta una de las siguientes acciones: 2.1. Si el especialista escoge la opción de adicionar un nuevo reporte en el sistema se ejecuta el CA1 2.2. Si el especialista escoge la opción de modificar los datos de un reporte en el sistema se ejecuta el CA2 2.3. Si el especialista escoge la opción de ver los datos de un reporte específico en el sistema se ejecuta el CA3 2.4. Si el especialista escoge la opción de eliminar un reporte específico en el sistema se ejecuta el CA4
Flujo alternativo	**CA1. Insertar**

Figura 2.4: Modelo de caso de uso del sistema



2.3. Análisis y diseño del Sistema

Esta disciplina define la arquitectura del sistema y tiene como objetivos trasladar requisitos en especificaciones de implementación, al decir análisis se refiere a transformar casos de uso en clases, y al decir diseño se refiere a refinar el análisis para poder implementar los diagramas de clases de análisis de cada caso de uso, los diagramas de colaboración de cada caso de uso, el de clases de diseño de cada caso de uso, el de secuencia de diseño de caso de uso, el de estados de las clases, el modelo de despliegue de la arquitectura Chacón (2006).

2.3.1. Diagramas de Clases del Diseño

Un diagrama de clases del diseño representa la estructura estática del sistema con las clases, atributos, operaciones y relaciones que van a ser diseñadas e implementadas. Se incorporan en las clases del Modelo de Análisis / Diseño del Negocio atributos y responsabilidades u operaciones a un nivel alto de abstracción, y se etiquetan las clases con un estereotipo para categorizar las clases como interfaz, entidad o control **?**.

En la 2.5 se muestra el diagrama de diseño <<Gestionar Trabajadores>>. Escenario <<Insetar Trabajador>>.

En la 2.6 se muestra el diagrama de diseño <<Gestionar Categorías>>. Escenario <<Insetar Categoría>>.

En la 2.7 se muestra el diagrama de diseño <<Gestionar Subcategorías>>. Escenario <<Insetar Subcategoría>>.

Figura 2.5: Diseño de clases <<Insertar Trabajador>>

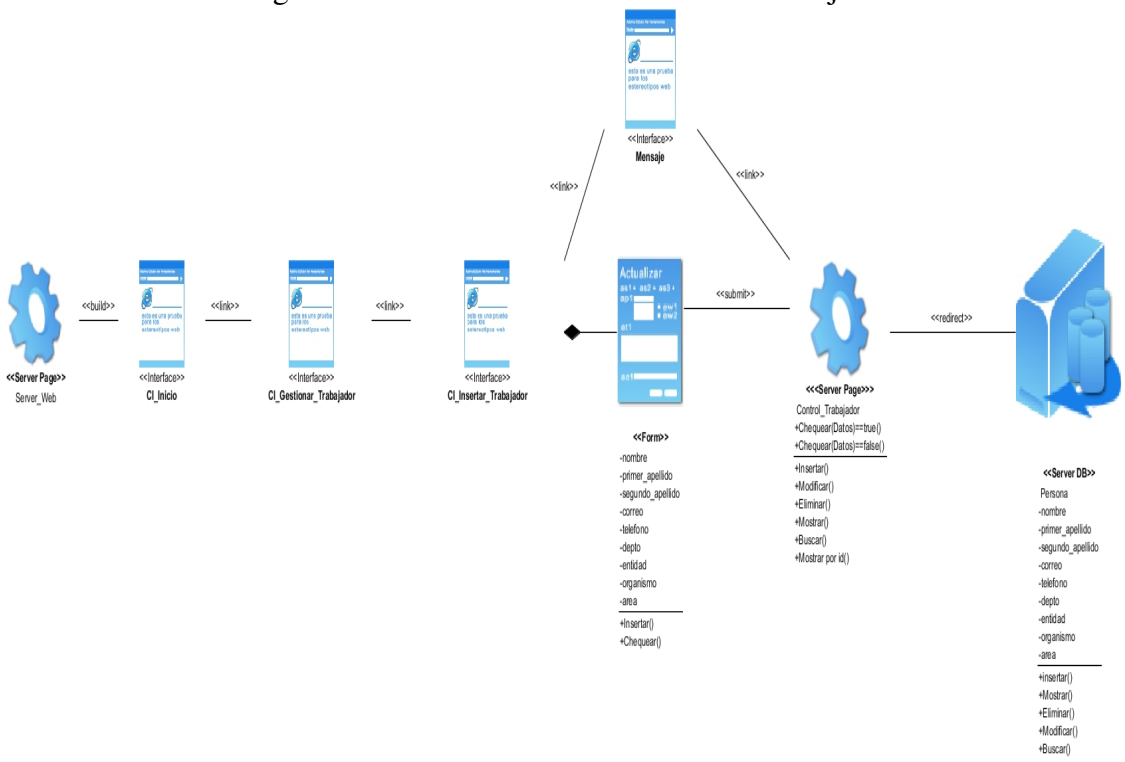


Figura 2.6: Diseño de clases <<Insertar Categoría>>

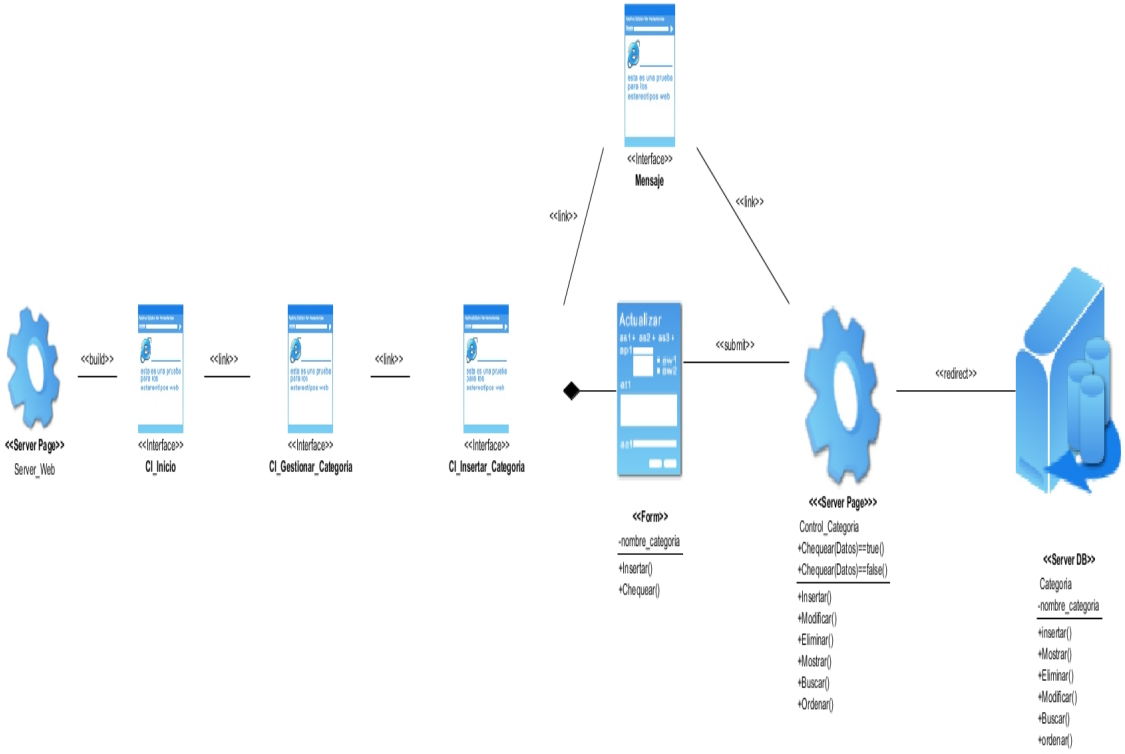
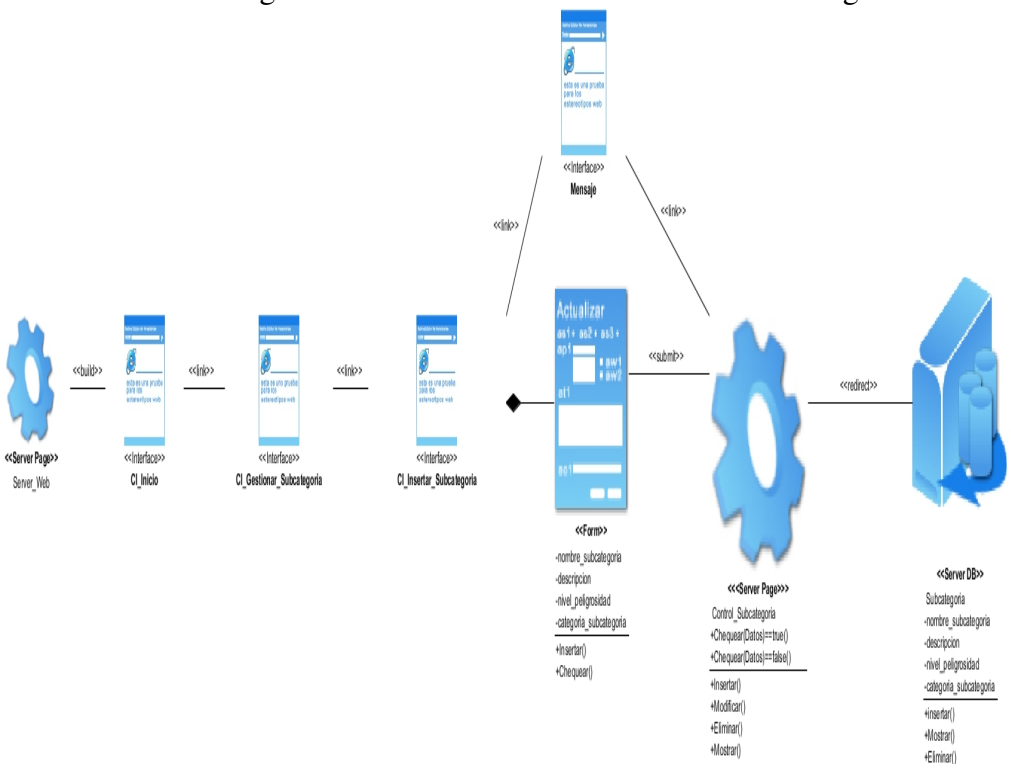


Figura 2.7: Diseño de clases <<Insertar Subcategoría>>



2.4. Diseño de la base de datos

En la siguiente Figura 2.8 se presenta el diagrama entidad-relación del sistema propuesto.

Todos los datos de la aplicación serán almacenados en una misma base de datos estructurada por tablas. En la figura 2.9 se muestra el diagrama físico de la base de datos.

2.5. Conclusiones parciales

En este capítulo se muestra cómo funcionan el negocio y el sistema a través de los artefactos proporcionados por la metodología RUP. Además, se obtuvo una descripción general del sistema identificando los requerimientos funcionales y no funcionales, las reglas y los procesos del negocio. La construcción de todos estos artefactos propició que se esclareciera cómo

es el flujo de eventos que se realiza en cada uno de los procesos del negocio y se establecieran las relaciones de cada uno de los actores del sistema con las diferentes funcionalidades a implementar.

Figura 2.8: Diagrama Entidad-Relación

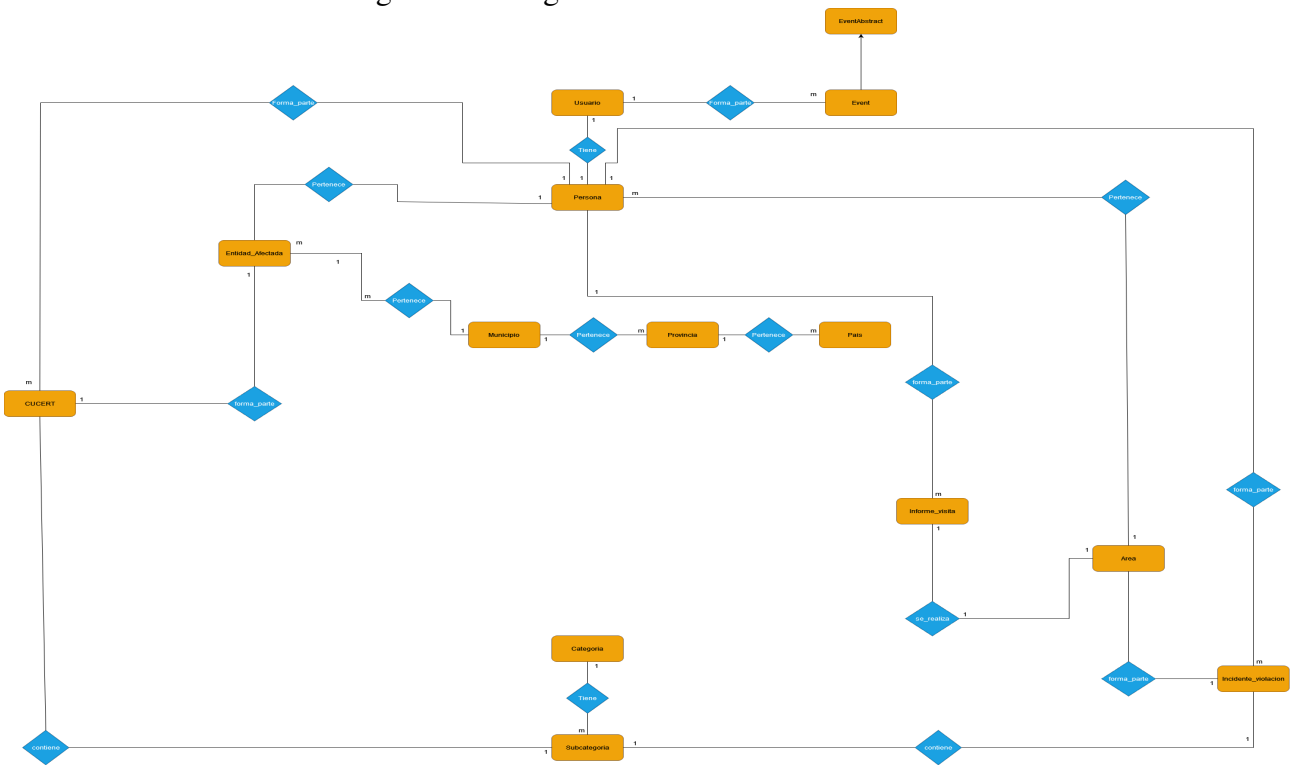
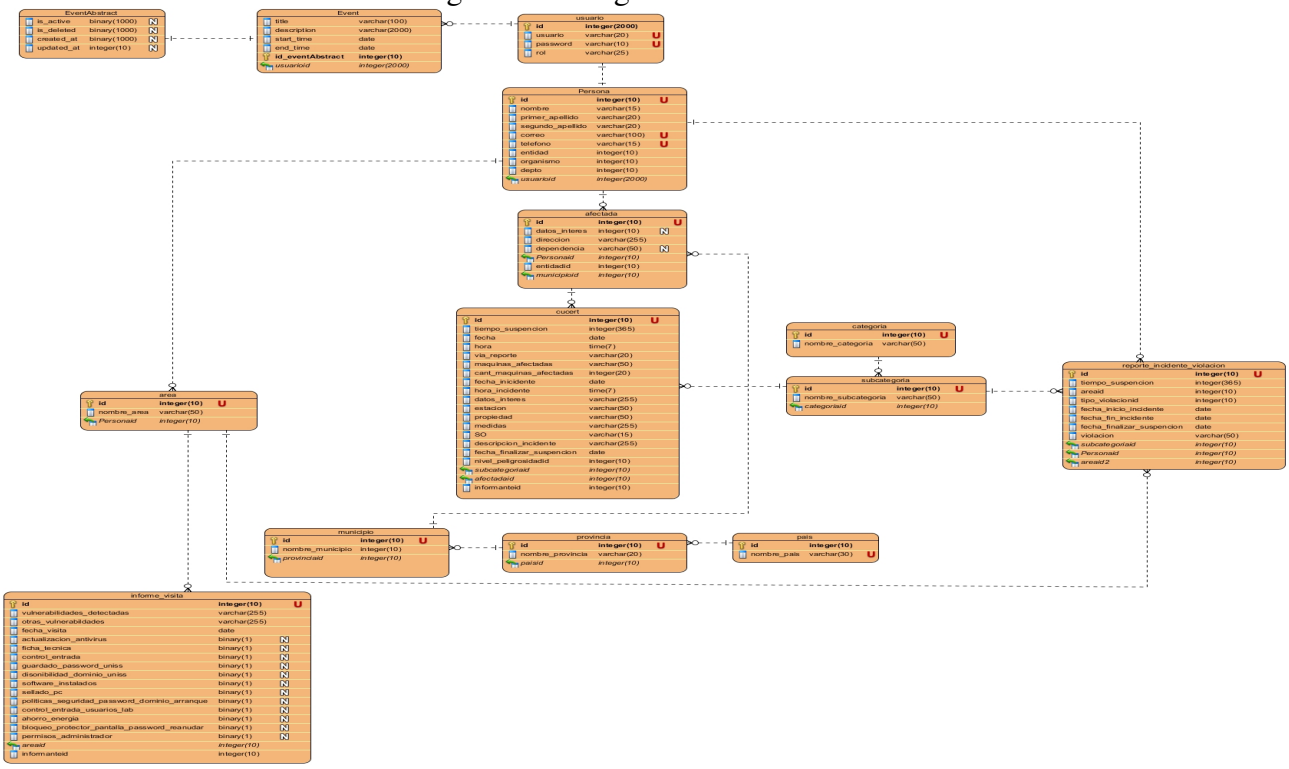


Figura 2.9: Diagrama Físico



CAPÍTULO 3

Desarrollo de un sistema informático para la gestión de los reportes de incidentes de la seguridad informática en la Universidad de Sancti Spíritus «José Martí Pérez»

En este capítulo se utiliza la metodología de desarrollo RUP para mostrar el proceso de desarrollo del sistema. Se detallan los temas de seguridad, diseño de la aplicación y tratamiento de los errores. Finalmente se realizan las pruebas unitarias, para el caso de uso más importante: Gestionar reporte CUCERT.

3.1. Ayuda, tratamiento de errores y seguridad

Para la realización del sistema, se deben tener en cuenta una serie de aspectos que determinen que el producto quede finalmente con la calidad deseada. Los principales, en este caso, son la ayuda del sistema, su seguridad y el tratamiento a los errores. Los mismos serán detallados a continuación.

3.1.1. Ayuda

Habrá un documento en formato Word con el nombre <<Manual de Usuario>> donde se explicará paso a paso lo necesario para el despliegue la ejecución y el funcionamiento de la aplicación.

3.1.2. Tratamiento de errores

Para el proceso de implementación del sistema, se procuró evitar la mayor cantidad de errores y excepciones posibles. Para ello se aprovecharon las ventajas del framework Django, y se validó que la información a introducir por los usuarios al momento de gestionar cuente con el formato correcto, para así evitar que se generen excepciones.

En caso de que no fuese posible realizar lo anterior, se provee a la aplicación de mensajes de error que siguen las siguientes reglas:

- Utilizar el mismo formato en todos los mensajes para lograr una consecuencia entre los errores y una detección casi intuitiva del error.
- No culpar al usuario del problema ocurrido.
- Escribir los mensajes de error de modo que sean comprensibles para el usuario.

3.1.3. Seguridad

En el sistema, la seguridad se gestiona mediante la autenticación de usuarios. Inicialmente debe registrarse el usuario insertando correctamente los datos necesarios, lo que le permitirá acceder a las opciones de administración brindadas en el software.

Existe un rol de usuario llamado «admin» que será el único autorizado a gestionar el módulo de usuarios y registrar los mismos.

Existe un rol de usuario llamado «usuario» que las únicas acciones que podrá hacer serán leer las noticas de ciberseguridad y escanear un url, una vez que el «admin» registre a los usuarios.

Los usuarios solo tendrán acceso a las opciones que le sean permitidas en dependencia del rol al que pertenezcan.

3.2. Prototipos de interfaz de usuarios

En la figura (capturas de pantalla del software)

En la figura 3.1 se muestra la interfaz de usuario de autenticación.

En la figura 3.2 se muestra la interfaz inicial (la página de inicio) con el servicio RSS de noticias de Ciberseguridad.

En la figura 3.3 se muestra la interfaz de los trabajadors insertados en el sistema.

En la figura 3.4 se muestra el formulario de insertar un trabajador.

En la figura 3.5 se muestran las opciones de eliminar, modificar y ver los datos más detallados del trabaja.

Figura 3.1: Autenticación

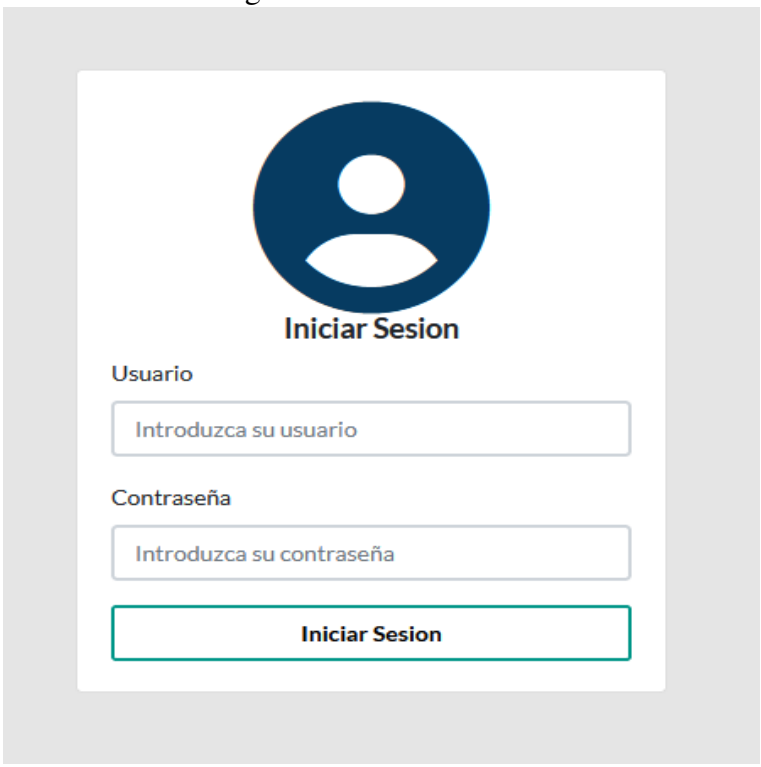


Figura 3.2: Inicio

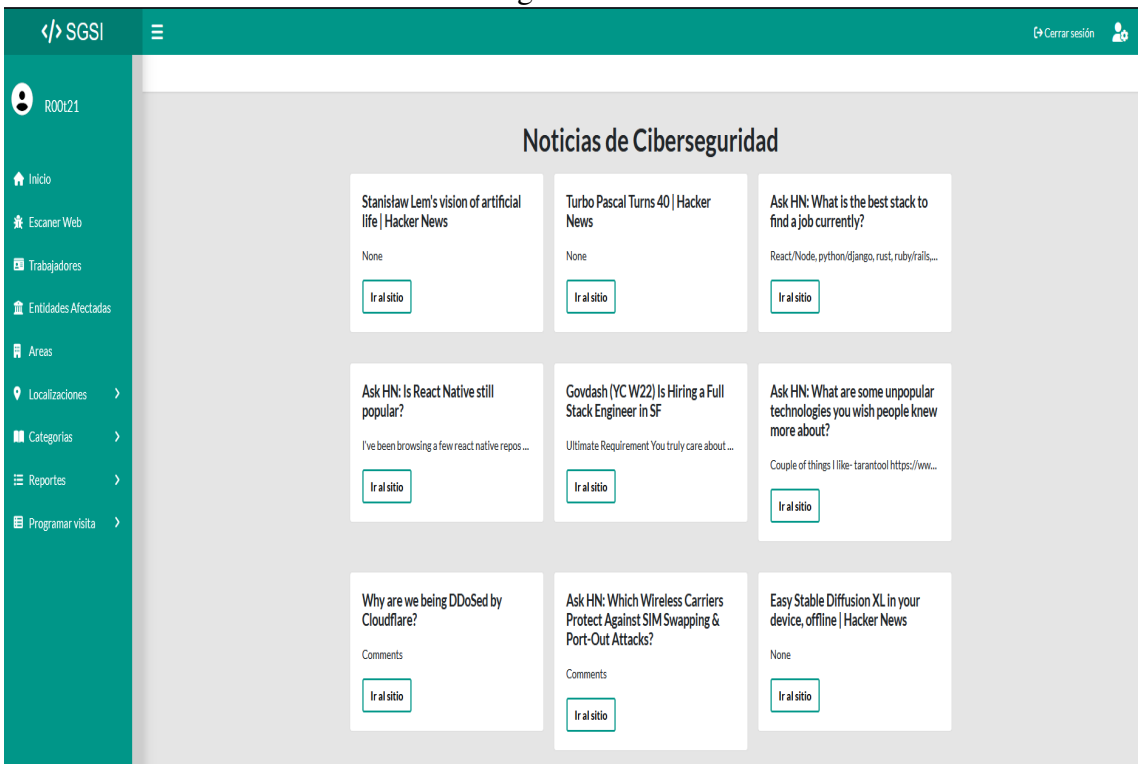


Figura 3.3: Trabajadores

Figura 3.4: Formulario insertar trabajador

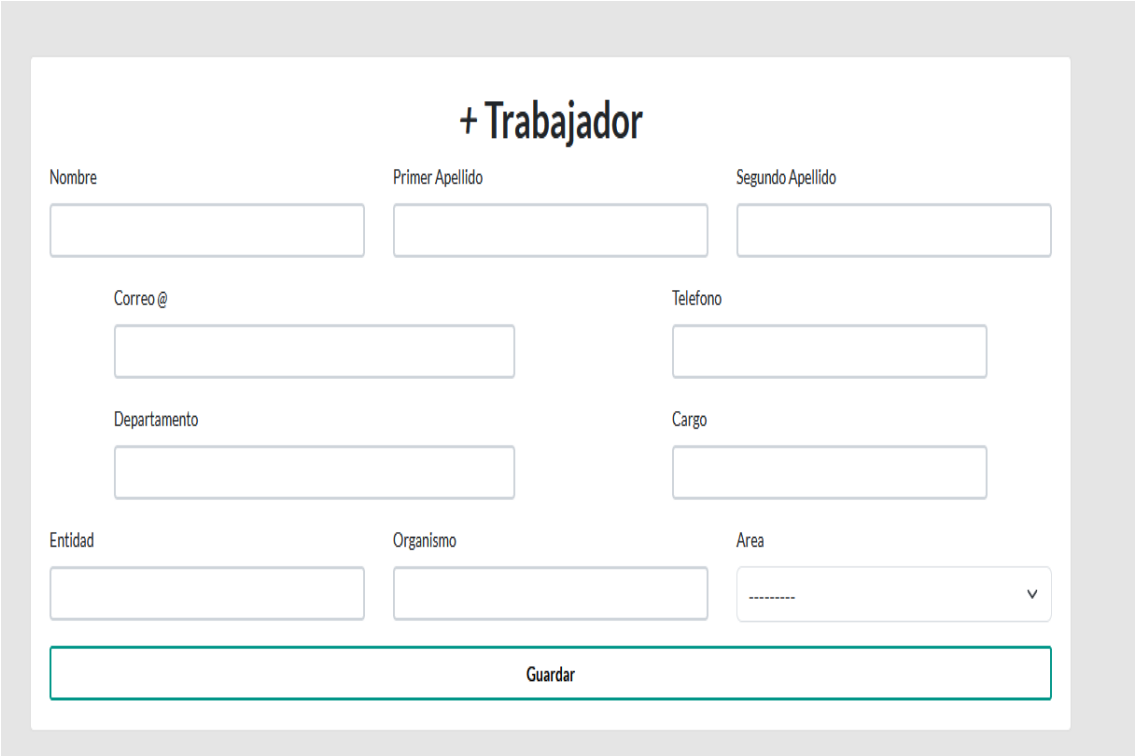


Figura 3.5: Detalle de trabajador

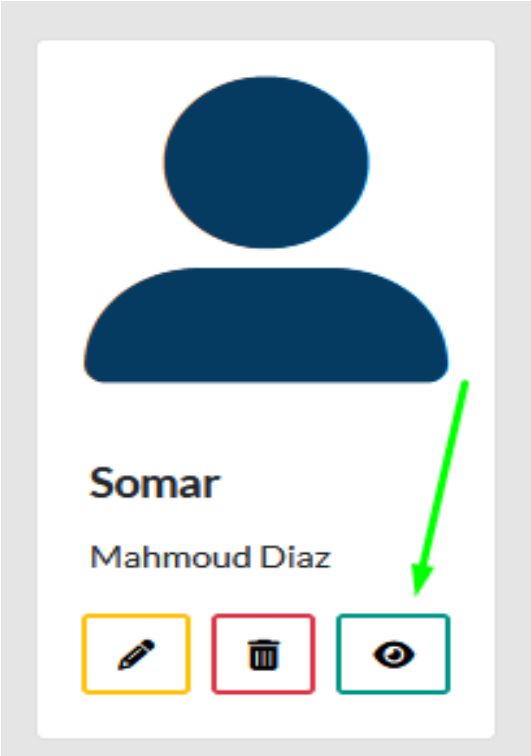
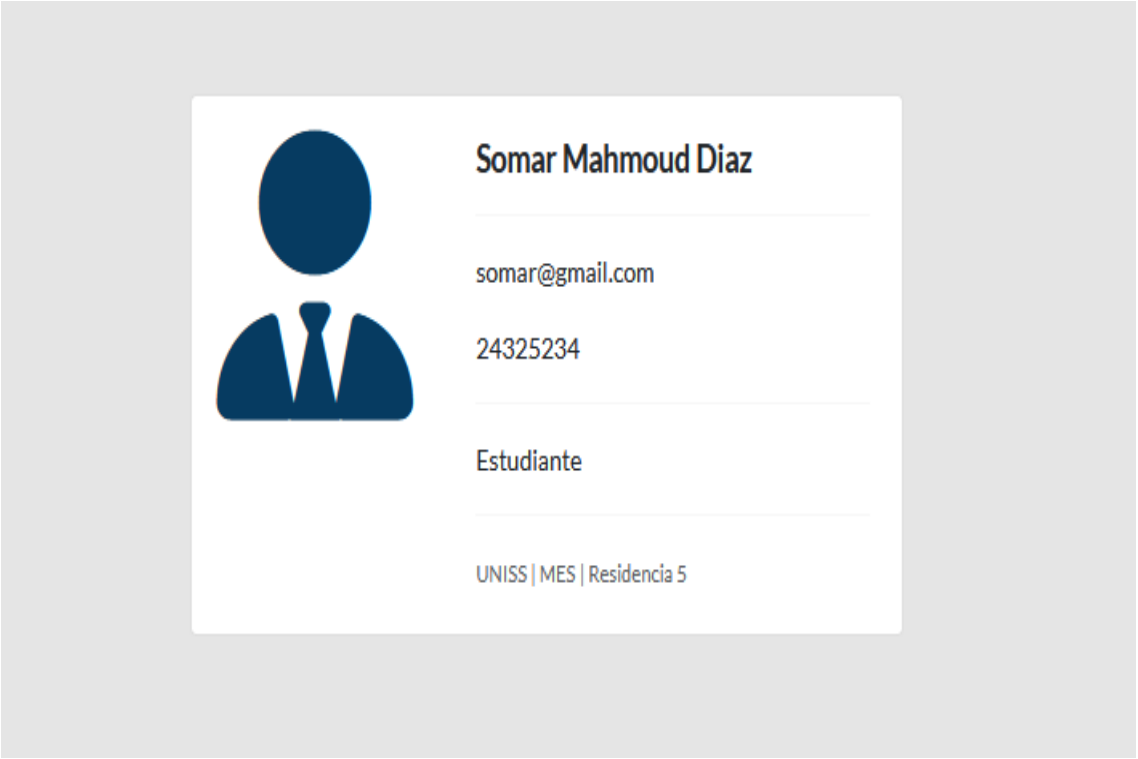


Figura 3.6: Trabajador Completo



3.3. Modelo de implementación

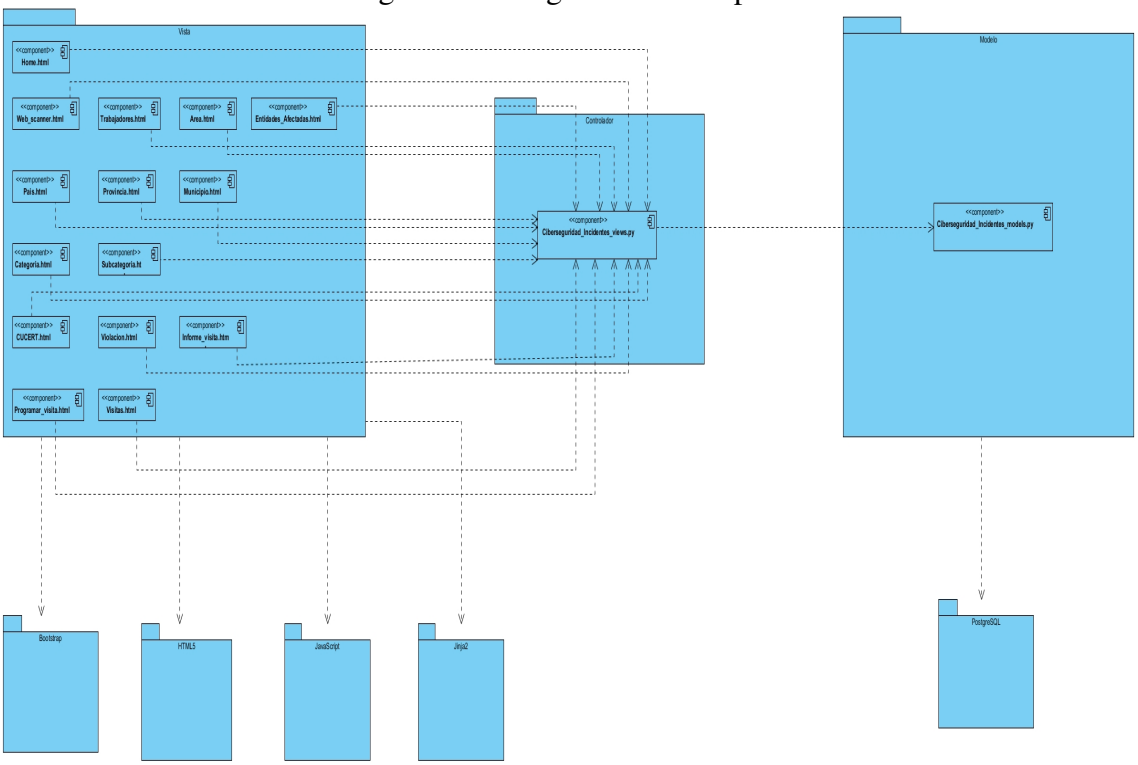
Es una colección de componentes, y de subsistemas de aplicación que contienen estos componentes, entre estos están los entregables, ejecutables, archivos de código fuentes Chacón (2006).

3.3.1. Diagrama de componentes

Un diagrama de componentes proporciona una visión general del sistema y documenta la organización de los componentes del mismo, sus relaciones y dependencias mutuas.

En la Figura 3.7 se muestra el diagrama de componentes del sistema ilustrando una visión general del mismo.

Figura 3.7: Diagrama de Componentes

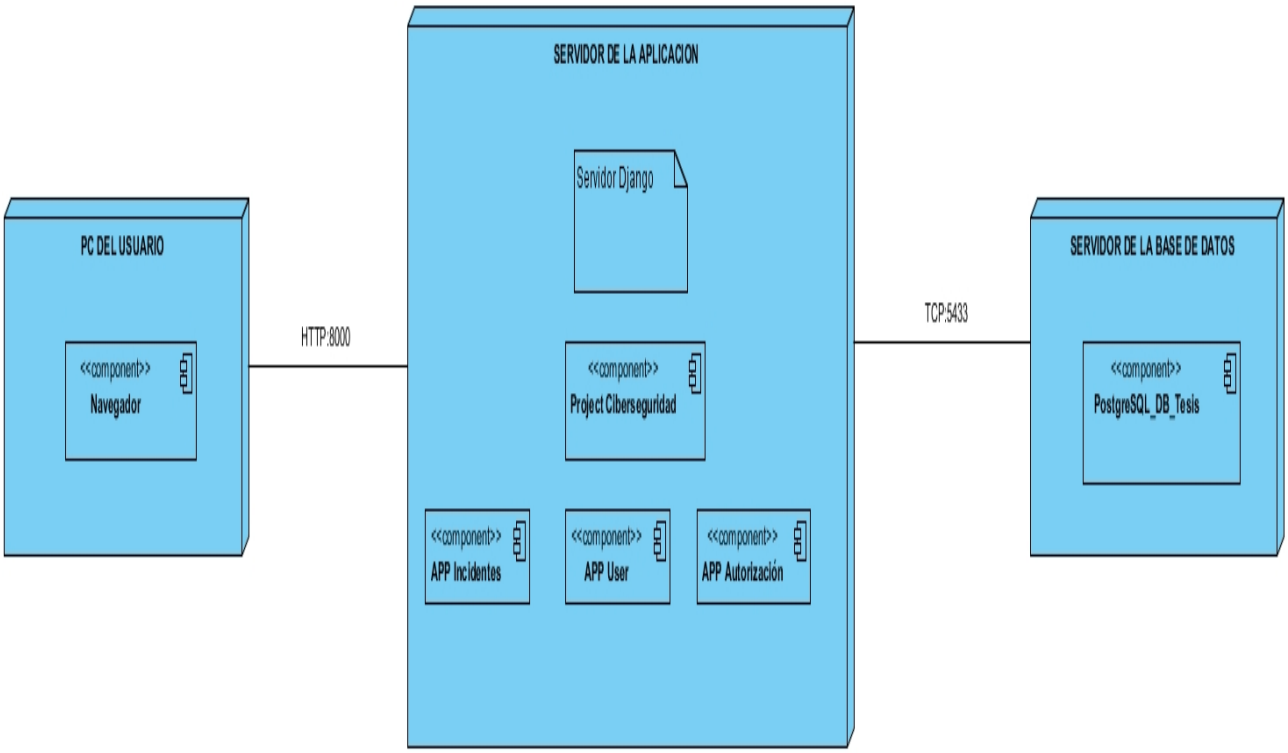


3.3.2. Diagrama de despliegue

Los diagramas de despliegue son diagramas estructurados que muestran la arquitectura del sistema desde el punto de vista del despliegue (distribución) de los artefactos del software en los destinos de despliegue. Los artefactos representan elementos concretos en el mundo físico que son el resultado de un proceso de desarrollo.

La Figura 3.8 muestra el diagrama de despliegue correspondiente al software.

Figura 3.8: Diagrma de Despliegue

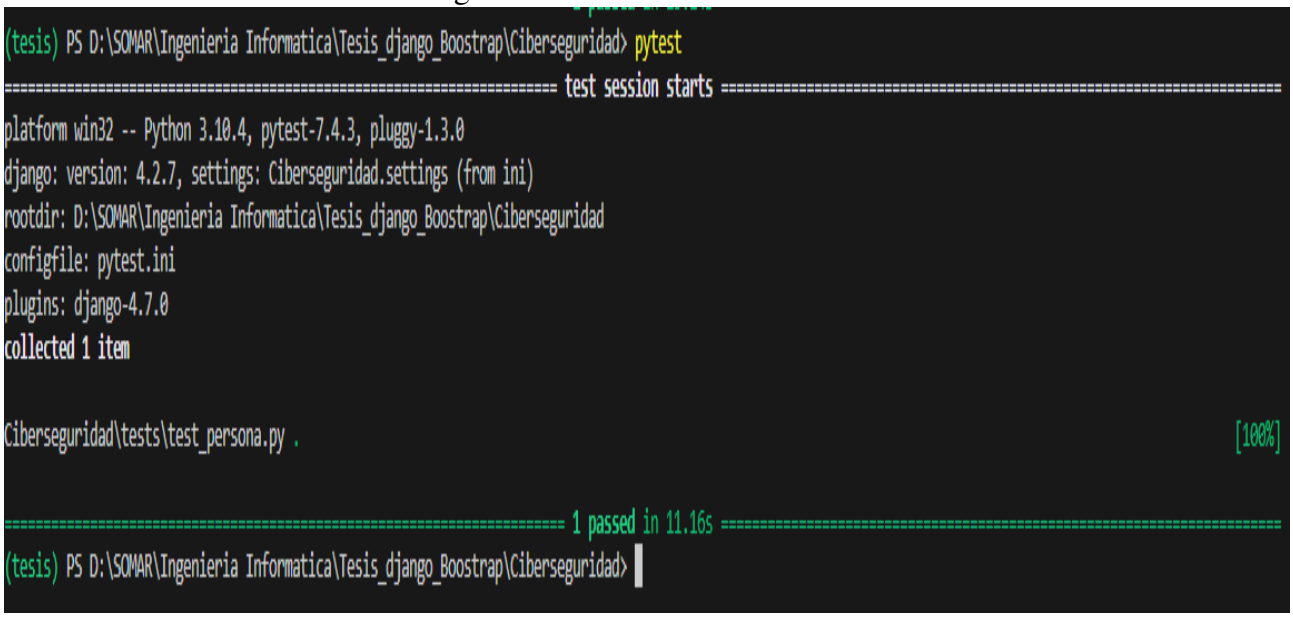


3.4. Pruebas Unitarias

Es como se comprueba el normal funcionamiento del código dentro de un programa, para la detección inmediata de defectos en métodos, mejor diseño detallado de la arquitectura. Código estructurado y menos complejo, documentación acorde a la realidad del aplicativo el tiempo invertido en el mantenimiento de la evolución Arias et al. (2018).

En la Figura 3.9 se muestra para el caso insertar Area, luego de introducir un conjunto de datos, estos se comparan con la base de datos, si están correctos emite un mensaje de satisfactorio con una puntuación de [100 %].

Figura 3.9: Prueba Unitaria



3.5. Conclusiones parciales

A través de este capítulo se explicó como son tratados en el sistema la ayuda al usuario, el tratamiento de errores y la seguridad. Mostrando los prototipos de interfaz. Se representó el diagrama de componentes y de despliegue y finalmente se llevó a cabo las pruebas unitarias realizadas al caso de uso «Gestionar Áreas».

CONCLUSIONES

CONCLUSIONES A partir del desarrollo del presente proyecto se concluye en lo siguiente:

1. El estudio de los fundamentos teóricos y metodológicos para la elaboración del sistema informático permitió determinar que la metodología RUP es la adecuada para desarrollo del mismo. Para el backend se seleccionó el lenguaje de programación Python como lenhuaje base con su framework de desarrollo Django y el sistema gestor de base de datos PostgreSQL.

2. Se diseñó un sistema para contribuir a la gestión de los incidentes de la seguridad informática en la Universidad de Sancti Spíritus «José Martí Pérez». Se esclareció cómo es el flujo de eventos que se realizan en cada uno de los procesos del negocio y se describió de manera general el sistema, identificando los requerimientos funcionales y no funcionales.

3. Se desarrolló un sistema con funcionalidades que se ajustan a las necesidades del cliente, y teniendo en cuenta el sistema la ayuda al usuario, el tratamiento de errores y la seguridad. Además, se validó el mismo para comprobar su correcto funcionamiento.

RECOMENDACIONES

Se recomienda realizar un estudio experimental más amplio que permita comparar el comportamiento del método propuesto con otros métodos de aprendizaje multi-instancia que no transformen la representación multi-instancia.

Además, se recomienda utilizar el método propuesto en la solución de problemas reales en la gestión de los incidetnes de la seguridad informática.

También se recomienda hacer un sistema de notificaciones para el aviso del día y la fecha de una visita planificada y para el aviso a las personas adecuadas que sus cuentas que encuentren en estado suspendido por vá de correo o por un sistema de notificación propio en el sistema.

REFERENCIAS

Alvarado, R., Acosta, K., Buonaffina, Y. V., Alvarado, R., Acosta, K. y Buonaffina, Y. V. (2018). Necesidad de los sistemas de información gerencial para la toma de decisiones en las organizaciones, *InterSedes* **19**(39): 17–31. Publisher: http://creativecommons.org/licenses/by-nc-nd/3.0/.
URL: *http://www.scielo.sa.cr/scielo.php?script=sci_abstract pid = S2215 − 24582018000100017lng = ennrm = isotlng = es*

apd, s. (2020). Metodología Scrum: cómo aplicar el método Scrum | APD.
URL: *https://www.apd.es/metodologia-scrum-que-es/*

Arias, M. Á. (2017). *Aprende Programación Web con PHP y MySQL: 2ª Edición*, IT Campus Academy. Google-Books-ID: mP00DgAAQBAJ.

Arias, S. V., Soria, T. M., Moya, P. N. y Palma, P. M. (2018). Control de calidad del software mediante pruebas automatizadas de integración y pruebas unitarias, *Ciencia Digital* **2**(3): 101–115. Number: 3.
URL: *https://cienciadigital.org/revistacienciadigital2/index.php/CienciaDigital/article/view/140*

Asana (2022). ¿Qué es la programación extrema (XP)? [2022].
URL: *https://asana.com/es/resources/extreme-programming-xp*

C. G., T. y Devl, J. (2021). A Study and Overview of the Mobile App Development Industry | International Journal of Applied Engineering and Management Letters (IJAEML).
URL: *https://supublication.com/index.php/ijaeml/article/view/424*

Carley, K. M. (2020). Social cybersecurity: an emerging science, *Computational and Mathe-*

matical Organization Theory **26**(4): 365–381.
URL: *https://doi.org/10.1007/s10588-020-09322-9*

Chacón, J. C. R. (2006). Aplicación de la metodología RUP para el desarrollo rápido de aplicaciones basado en el estándar J2EE, *Guatemala:(tesis de grado) para obtener el título de ingeniería en ciencias y sistemas-Universidad de San Carlos de Guatemala* .

ANEXO A

Requisitos Funcionales

Tabla A.1: Requisitos funcionales (Cuadro Completo)

Requisitos funcionales (Cuadro completo)

R 10.5	Mostrar subcategoría específica
Nº	Requerimientos
R 1.0	Autenticar usuario
R 2.0	Gestionar usuario
R 2.1	Insertar usuarios
R 2.2	Modificar usuarios
R 2.3	Eliminar usuarios
R 2.4	Mostrar usuarios
R 3.0	Gestionar tranajadores
R 3.1	Insertar trabajadores
R 3.2	Modificar trabajadores
R 3.3	Eliminar trabajadores
R 3.4	Mostrar trabajadores
R 3.5	Mostrar trabajador especifico
R 4.0	Gestionar entidades afectadas
R 4.1	Insertar entidades afectadas
R 4.2	Modificar entidades afectadas
R 4.3	Eliminar entidades afectadas