DESARROLLO DE UN OBJETO VIRTUAL DE APRENDIZAJE (OVA) PARA EL DIAGNÒSTICO Y SEGUIMIENTO DE VULNERABILIDADES EN UNA RED INALÁMBRICA WI-FI

JHONATHAN SÁNCHEZ CARRILLO
JORGE ALBERTO CASTIBLANCO

UNIVERSIDAD DE SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2010

DESARROLLO DE UN OBJETO VIRTUAL DE APRENDIZAJE (OVA) PARA EL DIAGNÓSTICO Y SEGUIMIENTO DE VULNERABILIDADES EN UNA RED INALÁMBRICA WI-FI.

JHONATHAN SÁNCHEZ CARRILLO
JORGE ALBERTO CASTIBLANCO

Proyecto de Grado como requisito para optar al título de Ingeniero de Sistemas

Asesora:
Msc. Olga Lucía Roa Bohórquez

UNIVERSIDAD DE SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
PROYECTO DE GRADO
BOGOTÁ D.C.
2010

Nota de aceptación:

_____

_____
_____
_____
_____
_____

_____
Firma Presidente del Jurado

_____
Firma del Jurado

_____
Firma del jurado

Bogotá D.C 2 de Noviembre de 2010

AGRADECIMIENTOS

Los autores queremos expresar nuestra más sincera gratitud a nuestros padres, profesores y especialmente a Dios, que es la fuerza y fortaleza para seguir adelante en los largos caminos que ofrece la vida.

También queremos agradecer a la Universidad San Buenaventura (Bogotá) y a todas las personas que colaboraron para la elaboración del “Objeto virtual de aprendizaje sobre el diagnóstico y seguimiento de vulnerabilidades en redes Wi-Fi.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

INTRODUCCIÓN

Las nuevas tecnologías aplicadas a la educación son temas que se escuchan frecuentemente, sin embargo esto no se reduce al uso de motores de búsqueda o la implementación de recursos estáticos que no permitan una integración de conocimiento por parte de alumnos. Las nuevas tecnologías tienden a la utilización de esquemas dinámicos que fortalezcan lo aprendido en aulas de clase.

Teniendo en cuenta lo anterior, el proyecto se basa en la elección de un medio virtual que permita la reutilización de contenidos y refuerce conceptos aprendidos por los investigadores. A través del desarrollo de un Objeto Virtual de Aprendizaje (OVA), la interacción entre alumnos y docentes se hace de forma más equilibrada, el docente ya no solo se limita a la presentación de temas, a su vez los alumnos deben apoyar y reforzar los contenidos del curso.

Un OVA es un mediador educativo que permite a los interesados en un tema, interactuar dinámicamente para obtener conocimientos. Este recurso tecnológico, se convierte poco a poco en una herramienta útil para el desarrollo educativo y para la creación de nuevas estrategias de aprendizaje en alumnos.

En Colombia los Objetos Virtuales de Aprendizaje (OVAs), son relativamente nuevos y a través del Ministerio de Educación Nacional se han liderado procesos de incorporación en diversos centros educativos como herramienta de apoyo a la docencia.

El objetivo de este proyecto es implementar un Objeto de Aprendizaje (OVA) para el diagnóstico y seguimiento de vulnerabilidades en redes inalámbricas WI-FI. La ventaja que ofrece esta nueva estrategia de aprendizaje, es la manera explícita del contenido publicado. Esto quiere decir que el alumno puede acceder a la información por medio de documentos, videos, imágenes, lecturas, opiniones y a su vez permite retroalimentar el sistema, para el uso posterior de dicho material.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES (ESTADO DEL ARTE)

Desde que las redes de ordenadores fueron creadas en la década de los años setenta, surgieron grandes ventajas en cuanto a comunicación se refiere. Sin embargo no se tenían muchas medidas para proteger la información. Como dice Jeimy Cano[1] el nacimiento de las primeras redes de comunicación, garantizaban el intercambio de información, pero no contaban con un sistema robusto de seguridad.

Para el Dr. Jeimy Cano J. La falta de conocimiento sobre la seguridad informática, implica que las vulnerabilidades que atacan los sistemas de información, se hagan cada vez más evidentes y se incremente la perdida de información.

La gestión y administración de un negocio, se basa en los datos y en la información que se maneje. Esto no es ajeno a las entidades educativas que día a día, se fortalecen con métodos más efectivos, para proteger su información. Como expone Alberto J.E.Piatelli Piraud [2] en su artículo "Algunas claves para el éxito en la Toma de Decisiones Gerenciales" se definen tres tipos de información:

Información de alta prioridad: Se identifica por ser confidencial y es responsabilidad exclusiva de los miembros que intervienen en ella. Es vital para los intereses de la empresa, porque en ellos se establecen las directrices del negocio.

Información de mediana prioridad: Se caracteriza por contener datos que no son vitales para la compañía pero que son de uso exclusivo para los interesados.

Información de Baja Prioridad: Se caracteriza por que su importancia tiene un poder relevante en la organización, es decir que no actúan directamente en los procesos fundamentales de la empresa. Este tipo de información puede ser vista por cualquier miembro de la compañía.

[1] CANO, Jeimy J. Ph.D Gestión de la Inseguridad informática. Bogotá: Abril-junio 2008. P.11
[2] . J.E.Piatelli Piraud Alberto. Marzo de 2008. [En línea]. [Consulta: Agosto 26 de 2009]. Disponible en: <http://www.formaciononline.org/noticias/016_claves_exito_gerencial.htm>

Se puede decir que la información es parte esencial en cualquier organización, y que dependiendo la forma de administrarla, se puede llegar al éxito o fracaso de la compañía.

Según el artículo "Gestión de la inseguridad informática", del autor Cano Jeimy J, se puede destacar lo siguiente:

> La industria de la seguridad, la constante evolución de las vulnerabilidades y la psicología de la seguridad son componentes que interrelacionados nos permiten avanzar en el reto de conocer la inseguridad de la información, no para llegar a comprenderla totalmente, sino para reconocer en sus tendencias y conexiones una forma para mejorar nuestras estrategias de preparación y respuesta a incidentes.
>
> Avanzar en la gestión de la seguridad de la información, es conquistar nuestro temor natural por la inseguridad, por la materialización de los riesgos:[3] …

Según el libro HACKING Y SEGURIDAD EN INTERNET las vulnerabilidades y ataques a sistemas de comunicación son cada vez más frecuentes, gracias a la aparición de Internet. Hace unos años la mayoría de ataques se realizaban de forma local, es decir que por lo general los mismos miembros de la compañía eran los que atentaban contra la misma.

En la actualidad, los ataques van más allá de las redes LAN (*Local Área Network).* El libro afirma lo siguiente:

> "la llegada de Internet a los hogares de forma masiva, las comunicaciones virtuales, los foros de trabajo, la comunidad de código abierto, los conocidos gusanos informáticos que llaman a nuestras puertas de una manera cada vez más frecuente e incluso los medios de comunicación han impulsado el conocimiento de estos mundos, convirtiéndose en una realidad muy cercana para muchas personas.

[3] CANO, op.cit., p 11

> La falsa percepción de seguridad en los sistemas telemáticos que rigen nuestras vidas ha sido puesta en jaque múltiples veces. Los complejos sistemas informáticos que aseguran la continuidad de nuestra sociedad han tenido que ponerse a trabajar en seguridad para asegurar la confiabilidad de su funcionamiento. La red de redes ha llevado a manos de toda persona que lo desee herramientas desarrolladas por los verdaderos hackers, que eran inconcebibles apenas hace una década."[4]

Siguiendo con la investigación y la documentación existente sobre el tema de la seguridad en las redes informáticas, se pueden destacar los artículos Security Education Using Second Life y Digital Forensics de la revista IEEE (Institute of Electrical and Electronics Engineers)[5], en los cuales centran su atención sobre aspectos relacionados con la seguridad y privacidad de la información.

Es un tema extenso en el cual se exponen grandes características de las investigaciones sobre incursiones no autorizadas a sistemas de comunicación. La definición básica que se presenta es la siguiente:

> "una investigación digital es un proceso de resolver preguntas acerca de estados y eventos digitales pasados, donde un investigador digital forense, establece cual fue el proceso de acceso ilegal a una red y de esta manera aplica las leyes vigentes a los infractores." [6]

Basándose en lo anterior, se tiene una visión más amplia sobre la inseguridad informática, es por ello que el campo de acción que propone el proyecto se centra en la creación de un Objeto Virtual de Aprendizaje que ilustra y enseña a que riesgos y vulnerabilidades se enfrentan las redes informáticas en la actualidad. En un principio, el OVA va dirigido a los alumnos de la Universidad de San Buenaventura, sede Bogotá, aunque posteriormente será de uso particular, para aquellos que estén interesados en el tema.

Existen múltiples definiciones de lo que es un OVA, sin embargo en este documento se citará una que se emplea en el portal de Colombia aprende. Este sitio web es avalado por el Ministerio de Educacional Nacional de Colombia, y

[4] PICOUTO, Fernando R. Hacking y seguridad en Internet. México: diciembre 2007. p.15.
[5] CARRIER Brian D. IEEE SECURITY AND PRIVACY, Artículo: Security Education Using Second Life. Piscataway, NJ, USA: Abril de 2009. p.45
[6] Ibíd., p.49.

busca fomentar la utilización de Objetos virtuales de aprendizaje. La definición dice lo siguiente:

> "Todo material estructurado de una forma significativa, asociado a un propósito educativo y que corresponda a un recurso de carácter digital que pueda ser distribuido y consultado a través de la Internet se considera un Objeto Virtual de aprendizaje. Los recursos empleados en el OVA deben ser reutilizables, lo que se relaciona con su característica de acceso frente a barreras tanto técnicas como legales". [7]

A través de los años, los OVA han adquirido una gran trascendencia e importancia por lo siguiente:

- La integración de procesos educativos con las nuevas tecnologías, hacen que los OVA sean una herramienta práctica para el desarrollo personal y grupal de conocimientos, en un área determinada. Los OVA son considerados como herramientas robustas que permiten potenciar procesos de aprendizaje. La UNESCO (International Institute for Educational Planning) se ha comprometido a analizar y desarrollar temas relacionados con los Objetos Virtuales de aprendizaje.

- Los OVA permiten que se intervenga en su desarrollo, ya que su concepto y entorno aún está en construcción.

Los Objetos virtuales de aprendizaje (OVA) buscan integrar de una manera práctica y eficiente a los alumnos o personas que estén interesadas en un tema específico, para que de esta manera desarrollen sus conocimientos individuales.

Para la Universidad de San Buenaventura, se hace necesaria la creación de nuevos métodos educativos, los cuales promuevan el aprendizaje en los alumnos e investigadores. Como se explicaba anteriormente, los OVAs son un medio útil para la utilización de contenidos virtuales, con fines académicos. El Ministerio de Educación de Colombia fundamenta una parte de sus investigaciones en dicho tema.

[7] OBJETOS VIRTUALES DE APRENDIZAJE. Enero de 2009. [En línea].[Consulta: Octubre 23 de 2009]. Disponible en: http://www.ucc.edu.co/Documents/06%20OBJETOS%20VIRTUALES%20DE%20APRENDIZAJE.pdf /

Según el artículo "Seguridad informática en Colombia"[8], Tendencias 2008, del autor Jeimy Cano, se realizó una encuesta en la cual se analizaron diferentes sectores productivos del país sobre la seguridad de la información. Este artículo de la Seguridad informática en Colombia, se hace necesario para el enfoque del proyecto, ya que el OVA va relacionado directamente con la protección de la información en las redes de comunicación y puede orientar sobre el análisis y la realidad que afrontan las organizaciones a la hora de proteger sus datos.

El análisis presentado en dicho estudio se basó en una muestra aleatoria que respondió una encuesta de tipo virtual, a través de una página Web de la Asociación Colombiana de Ingenieros de Sistemas ACIS. (Ver anexo C).

Comparando los resultados obtenidos en la encuesta del año 2008, con un estudio realizado en el año 2010 titulado "Encuesta nacional Seguridad informática en Colombia: Tendencias 2010", se muestra la evolución que han tenido algunos aspectos para la protección de datos.

Según Andrés Ricardo Almanza Junco[9], se observa un gran esfuerzo por prevenir ataques a las redes informáticas, considerando la panorámica latinoamericana. Países como México, Argentina, Paraguay y Uruguay han realizado este tipo de estudios para determinar el grado de compromiso que tienen algunos sectores productivos, con la seguridad de la información.

Este año la decima encuesta Nacional de Seguridad de Informática contó con la participación de 194 personas de diversos sectores productivos del país. Así como en el año 2008 este estudio evaluó las siguientes características:

- Demografía.
- Presupuestos.
- Fallas de seguridad.

[8] CANO, op.cit., p. 38.
[9] ALMANZA, Andrés R. Seguridad de la Información. ACIS. Bogotá: Mayo - Julio 2010 p 26.

- Herramientas y prácticas de seguridad.
- Políticas de Seguridad.
- Capital Intelectual.

Las conclusiones generales de esta encuesta fueron:

- Como en la encuesta del 2008, la mayor inversión en seguridad está enfocada a las tecnologías como las redes y sus componentes. En comparación con el estudio del 2010, se ve un ligero incremento por la protección de la propiedad intelectual y derechos de autor.

- Las principales causas para invertir en seguridad son la continuidad del negocio, normatividades y reputación de las organizaciones.

- Según las normas nacionales e internacionales, Colombia tendrá una evolución significativa a la hora de fortalecer los sistemas de gestión de seguridad.

- Comparando la encuesta del 2008 y 2010, la tendencia de dos años mínimos de experiencia en el campo de la seguridad de la información continua siendo un requisito.

- Certificaciones como la CISSP,CISA y CISM son las más valoradas por las organizaciones, a la hora de nuevas contrataciones.

- Al igual que el 2008, los medios más utilizados para proteger la información son los antivirus, contraseñas, firewalls de software y de hardware. Se ve un incremento considerable en implementación de certificados digitales.

- Los virus continúan siendo el mayor mecanismo de inseguridad en las redes informáticas. Sin embargo no se presta mucha atención a este tipo de ataques.

- Aunque existan leyes en contra de delitos informáticos, aún es difícil llevar un proceso judicial debido a los grandes costos que puedan generar.

- Se necesita mayor compromiso por parte de las organizaciones para adoptar políticas de seguridad confiables, que permitan mayor control en los dispositivos de red y control de la información.

- Los estándares internacionales están siendo implementados en Colombia. Entre estos estándares se destacan el ISO 27000, ISO 27001, ISO 27002 y las guías del NIST.

Es necesario hacer una proyección a largo plazo que presente los posibles cambios que pueda tener la seguridad de las redes informáticas. Según el artículo "La seguridad de la información en la década 2010-2020", de la revista Sistemas, el autor Roberto Arbeláez[10] hace unas reflexiones personales sobre la evolución que tendrá la protección de la información a lo largo de una década.

En dicho artículo el autor expresa que la seguridad de la información está ligada a la evolución de la tecnología. Si se analizan detenidamente las proyecciones que hacen los expertos, es posible determinar a qué riesgos se enfrentaran los sistemas informáticos.

Un ejemplo puede ser la telefonía móvil. Hoy en día estos artículos juegan un papel muy importante, debido a la conexión inalámbrica que estos poseen. Según las características que se puedan presentar en el año 2015-2020 el uso masivo

[10] ARBELÁEZ, Roberto. Seguridad de la Información. ACIS. Bogotá: Mayo - Julio 2010 p 26.

de estos dispositivos será total, debido a los bajos precios que tendrán en el mercado y a la variedad de servicios con que contarán.

Teniendo esto como referencia, la telefonía móvil mostrara un incremento significativo en ataques y riesgos de seguridad, tanto físicos como lógicos. En la actualidad es difícil ver que los celulares multipropósito cuenten con antivirus, pero en 10 años será extraño encontrar este tipo de dispositivos sin este tipo de protección.

Según los analistas de tecnología, en unos años la telefonía móvil desplazará los equipos de cómputo, debido a la movilidad que estos presentan y los servicios que estarán disponibles para comercio electrónico, banca, entre otros.

Este tipo de plataformas serán vulnerables a nuevos vectores de ataque si no se crea conciencia rápidamente, sobre el uso de estrategias confiables de seguridad en dichos dispositivos.

La infraestructura de seguridad proyectándola a 10 años, funcionará de manera integrada entre software y hardware. Por ejemplo los sistemas operativos, firewalls, antivirus deben ser integrados con componentes de trafico de red, sistemas de detección de intrusos, componentes de monitoreo de servicios, entre otros.

Si ocurre un intento de fraude en la red, el dispositivo afectado será inmediatamente aislado, negándole servicios, ejecución de aplicaciones, acceso a los componentes de red y almacenamiento de información y emitiendo un evento que reporte el incidente.

En los artículos citados anteriormente, se evidencia que cada vez más, se hace imprescindible los conocimientos sobre el tema de la seguridad en redes, en este caso específico la seguridad en redes inalámbricas Wi-Fi. Por otro lado las

nuevas tecnologías pretenden migrar la educación a un ambiente virtual y brindar a los alumnos e investigadores nuevas herramientas de aprendizaje.

El desarrollo de un Objeto Virtual de Aprendizaje sobre el diagnóstico y seguimiento de vulnerabilidades en las redes inalámbricas Wi-Fi, es fundamentalmente un aporte pedagógico, que busca integrar los conocimientos de docentes, alumnos e investigadores.

La publicación del OVA se hace en el servidor de cursosenbogota.com. La URL de la plataforma educativa es http://www.cursosenbogota.com/usbbgova, sin embargo se descarta el portal de Colombia aprende, por tratarse de un servidor privado y por seguir una normatividad del Ministerio de Educación Nacional, en la que se establece que los materiales deben ser estudiados a fondo antes de ser publicados en la red.

1.2 DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA

Con el desarrollo de las redes Wi-Fi, Las vulnerabilidades y ataques a sistemas de comunicación son cada vez más frecuentes, debido a la aparición de Internet.

Las redes Wi-Fi son aún más vulnerables que las redes por cable, debido a la propagación de las señales en todas las direcciones. Esto hace que el acceso no autorizado por parte de intrusos, se haga de una forma más sencilla.

Los ataques que sufren las redes inalámbricas, son en la mayoría de veces realizados desde el exterior. Esto quiere decir que un intruso intenta acceder ilegalmente a la información por medio de internet y no se hace necesario la conexión a un punto de red, como ocurría en el caso de medios cableados.

Por otro lado, el incremento de errores (*bugs*) en algunos aplicativos, hacen que el software sea de cierta forma inseguro y presente debilidades para proteger los datos. Por ejemplo un atacante puede obtener datos vitales de la red inalámbrica y a partir de ese momento empezar a planear un vector de ataque.

Los errores (*bugs*) en el software, se pueden corregir mediante la instalación de actualizaciones o soluciones proporcionadas por los mismos creadores del aplicativo, sin embargo este tipo de actualizaciones no están disponibles de manera inmediata cuando se producen los errores y hacen que se corran riesgos mientras se desarrollan dichas actualizaciones.

Otro punto que debe ser evaluado dentro de las organizaciones, es la falta de conocimientos y compromiso por parte de algunos usuarios que hacen uso de la red informática, para mantener la seguridad en dichos medios de comunicación. Un ejemplo claro de este problema, es la divulgación de contraseñas a otros integrantes de la misma compañía, lo que puede generar accesos no autorizados en aplicaciones propias de la organización o accesos no autorizados a la misma red inalámbrica.

En la actualidad existen diversos tipos de atacantes, que de una u otra forma buscan un objetivo individual. Por ejemplo existen usuarios mal intencionados, que intentan generar fallas en las redes informáticas y provocar una denegación de servicios. Es importante reconocer los perfiles de este tipo de usuarios para identificar los riesgos que se corren y las posibles soluciones que se pueden adoptar, para prevenir dichos ataques.

Teniendo en cuenta lo anterior, se hace necesario conocer los mecanismos y sistemas que pueden proteger las redes Wi-Fi, para proporcionar unos niveles de seguridad superiores y garantizar el correcto funcionamiento de la red informática.

Es necesario que las empresas modernas cumplan con unos estándares de calidad, los cuales deben proporcionar ciertos criterios de protección en cuanto a riesgos y vulnerabilidades se refieren, brindando confiabilidad, integridad y rendimiento en el manejo de información. El primer paso para conocer y evaluar vulnerabilidades en una red inalámbrica, es por medio de la investigación y estudio de riesgos, en los cuales se establezcan los niveles básicos de seguridad para protección de una red Wi-Fi.

¿Cómo desarrollar un Objeto Virtual de Aprendizaje (OVA) para el diagnóstico y seguimiento de vulnerabilidades en una red inalámbrica Wi-Fi?

1.3 JUSTIFICACIÓN

La seguridad en las redes informáticas, juega un papel prioritario, para prevenir ataques e incursiones no autorizadas, a los sistemas de información.

Por este motivo, el proyecto se caracteriza por dar una serie de conceptos y conocimientos sobre la seguridad informática, que podrá ser consultada por docentes, alumnos y en general toda aquella persona que está interesada en el tema.

Teniendo la idea anteriormente mencionada el proyecto tendrá como objetivo exponer los diversos componentes, ya sean de software o hardware que intervienen en la seguridad de la información. Todo esto se realizará por medio de un OVA con el fin de desarrollar un esquema de aprendizaje sencillo pero efectivo, que le permita al investigador, conocer a fondo lo relacionado con seguridad en redes informáticas.

El OVA que se plantea será única y exclusivamente para la Seguridad en redes inalámbrico. Se desea trabajar en este tema porque se considera fundamental

para la evolución y mantenimiento de cualquier tipo de negocio, que maneje información a través de una red. El proyecto pretende dar una visión clara sobre la importancia de la seguridad informática, conocer herramientas a nivel de hardware como *firewalls*, tratar temas tan prioritarios en la seguridad como *sniffers*, detectores de intrusos, encriptación, firmas digitales, claves asimétricas, claves simétricas, certificados digitales, entre otros.

Otra motivación para la realización del proyecto, es que la mayoría de investigaciones desarrolladas en OVAs han sido implementadas en el exterior. Colombia no puede ignorar los procesos educativos que permitan competencias y formación virtual. Por este motivo el Ministerio de Educación Nacional, ha dedicado importantes esfuerzos para incluir en estos procesos, sistemas virtualizados y en este caso, Objetos Virtuales de Aprendizaje.

El proyecto es factible de realizar en cuanto a información se refiere. Existen diversas fuentes que permiten conocer a fondo el tema de la seguridad informática. Entre dichos medios se destacan artículos, libros, informes, estadísticas, conferencias, medios digitales y documentación, estos son una fuente de información confiable para el desarrollo del OVA propuesto.

Otro aspecto importante, es que el proyecto permite el conocimiento a través de un modelo de virtualización, lo que genera una excelente alternativa de aprendizaje.

1.4 OBJETIVOS DE LA INVESTIGACIÓN

1.4.1 Objetivo General:

Objetivo General: desarrollar un Objeto Virtual de Aprendizaje (OVA) para el diagnóstico y seguimiento de vulnerabilidades en una red inalámbrica WI-FI, para facilitar el proceso de aprendizaje de los estudiantes, con el fin de adquirir la habilidad de prevenir incursiones no autorizadas a los sistemas de información y evitar posibles modificaciones o pérdidas de los datos.

1.4.2 Objetivos Específicos.

- Diseñar un OVA sobre seguridad en redes informáticas para facilitar el proceso de aprendizaje de los estudiantes.
- Determinar la metodología para la implementación del OVA propuesto en el proyecto.
- Desarrollar un Objeto Virtual de Aprendizaje, en el cual se especifiquen las principales características de la seguridad en las redes inalámbricas WI-FI.
- Desarrollar pruebas funcionales y de aceptación del OVA, definidas en el diseño del software.

1.5 ALCANCES Y LIMITACIONES

1.5.1 Alcances: el desarrollo del Objeto Virtual de Aprendizaje (OVA), pretende orientar a los alumnos de la Universidad de San Buenaventura (Bogotá), en el área de diagnóstico y seguimiento de vulnerabilidades en redes inalámbricas.

La plataforma contará con una función de autenticación que permitirá el acceso a los usuarios registrados y de esta manera ingresar a su perfil y las herramientas disponibles en el OVA. La aplicación también permitirá la administración de archivos como videos, documentos, comentarios. Pdfs, e imágenes publicadas por los administradores y usuarios.

1.5.2 Limitaciones: la publicación del OVA se hará en un servidor que soporte Objetos virtuales de Aprendizaje. En caso de no localizar dicho espacio dentro de la Universidad de San Buenaventura se propone buscar un servidor externo.

Otra limitación es la capacidad que ofrezca el servidor en el que se aloje el Objeto virtual de aprendizaje, para la publicación de contenidos y archivos necesarios para la interacción de los usuarios.

2. METODOLOGÍA

2.1 ENFOQUE DE LA INVESTIGACIÓN

Empírico-analítico: el interés de este enfoque se caracteriza por interpretar y transformar objetos del mundo material. Por medio de la experimentación, se buscan medios más confiables, a la hora de solucionar un problema. Este enfoque permitirá implementar un Objeto Virtual de Aprendizaje para el diagnóstico y seguimiento de vulnerabilidades en redes inalámbricas para fines educativos y fortalecimiento del proceso de aprendizaje en alumnos de la Universidad San Buenaventura (Bogotá).

3. LÍNEA DE INVESTIGACIÓN

3.1 LÍNEA DE INVESTIGACIÓN DE LA UNIVERSIDAD DE SAN BUENAVENTURA SEDE BOGOTÁ.

Tecnologías actuales y sociedad.

3.2 SUB LÍNEA DE LA FACULTAD DE INGENIERÍA.

Sistemas de Información y Comunicación.

3.3 CAMPO DE INVESTIGACIÓN.

Desarrollo de Software y Redes de Computadores.

4. MARCO DE REFERENCIA

4.1 MARCO TEÓRICO CONCEPTUAL

Las cifras de fraudes electrónicos a nivel mundial son un tema preocupante para la mayoría de organizaciones. El manejo de información es algo que se realiza cotidianamente en las compañías, sin embargo no se alcanza a dimensionar las vulnerabilidades de seguridad que se pueden presentar a lo largo de un dia de trabajo.

De acuerdo con un estudio realizado por la unidad de información empresarial (*The Economist Intelligence Unit*), titulado *Global Fraud Report ,* Colombia ocupa el segundo puesto en los países más victimizados por el fraude, sólo detrás de China y por delante de Brasil. El articulo expone lo siguiente:

> "Lo más preocupante de todo el panorama es que, según el estudio, ya ha causado que compañías nacionales dejen de crecer. Para rematar, el estudio prevé que las cosas empeoren.
>
> El fraude y el hurto de información por primera vez en la historia han superado los otros tipos de fraude en el mundo, y dice que "el 94% de los negocios colombianos sufrió algún fraude en el último año, en comparación con el 88% global". El 21% está en la categoría de fraudes electrónicos, que incluyen hurto de información y ciberataques (a sitios web e infraestructura de las empresas), y el porcentaje podría crecer en los próximos años"[11].

El Objeto Virtual de Aprendizaje para el diagnóstico y seguimiento de vulnerabilidades en las redes Wi-Fi, tiene como objetivo general, la integración de conocimientos entre alumnos, docentes e investigadores. El OVA desarrollado es un aplicativo virtual de uso pedagógico, que permite la gestión de diversos tipos

[11] IREGUI, Luis. Revista Enter. Octubre de 2010. [En linea]. [Consulta: Octubre 29 de 2010]. Disponible en: <http://www.enter.co/industria/colombia-es-subcampeon-mundial-en-fraude>

de archivos, para la comprensión de temas relacionados con la protección de la información en las organizaciones.

El desarrollo del aplicativo se hace mediante la utilización de software libre para administrar los contenidos publicados en dicha plataforma. Adicional a esto, se aplica el lenguaje de programación en JAVA para construir un simulador de redes inalámbricas Wi-Fi, el cual será un modulo del OVA.

En el OVA se encuentran 3 actores fundamentales que intervienen para la creación e integración de temas relacionados con la seguridad en las redes inalámbricas. Los actores que intervienen son:

- Estudiantes
- Docentes
- Administrador

Para modelar el sistema se emplea a UML (Lenguaje Unificado de Modelado) que junto al proceso de desarrollo de software RUP (*Rational Unified Process*), establecen la metodología estándar para la creación de aplicaciones. UML se trata de un lenguaje gráfico para construir, documentar, visualizar y especificar un sistema de software. UML también permite modelar los procesos del negocio, funciones, lenguajes de programación, manejo de información, entre otros. Existen tres categorías de diagramas para modelar un sistema, en este caso se especificará cada categoría con sus respectivos diagramas, para la elaboración del software.[12]

- **Diagramas de Estructura:** se modela mediante Diagrama de clases.

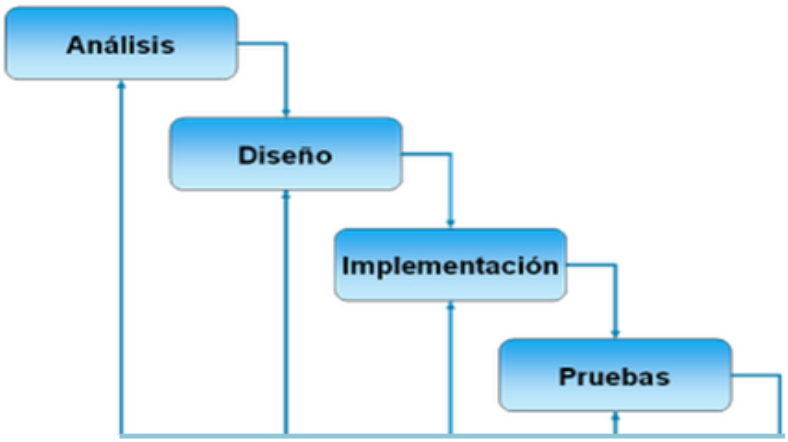
- **Diagramas de Comportamiento**: se modela mediante diagramas de casos de uso y diagramas de estado.

- **Diagramas de interacción:** se modela mediante diagramas de secuencia.

[12] ALEGSA, Definición UML. Enero 2010. [En línea]. [Consulta: Julio 6 de 2010]. Disponible en: <http://www.alegsa.com.ar/Dic/uml.php>

Para el desarrollo del software se aplica el método lineal. Este método está dividido por unas fases que permiten determinar el fin del proyecto. En el método lineal se encuentra el modelo en cascada el cual tiene una fase de análisis, diseño, implementación y pruebas. En la figura 1, se observa la secuencia de actividades para el modelo en cascada.

Figura 1. Diagrama del modelo en cascada.



Fuente: GALVIS, Edwin. Modelo en Cascada. Agosto de 2009. [En linea]. [Consulta: Octubre 15 de 2010]. Disponible en: <http://modeloencascada.blogspot.com/2009/08/diagrama-modelo-en-cascada.html >

Existen diversos tipos de modelos para el desarrollo del software, sin embargo se ha seleccionado el modelo en cascada, por estar divido en fases y permitir el desarrollo del proyecto de forma secuencial. Los modelos que se presentan son:

- Modelo en cascada.
- Modelo basado en prototipos.
- Modelo incremental o evolutivo.
- Modelo espiral.
- Modelo orientado a objetos.

En la tabla 1 se hace un comparativo entre los 4 primeros modelos de la anterior lista, donde se especifica el enfoque, ventajas, desventajas y aplicabilidad. Otra parte del proyecto consiste en la utilización de una herramienta gratuita, que permita administrar los contenidos, artículos, documentos y videos que se publiquen en el objeto virtual de aprendizaje.

Se ha seleccionado Joomla por tratarse de un sistema de gestión de contenidos, y entre sus principales virtudes está la de permitir editar el contenido de un sitio web de manera sencilla. Es una aplicación de código abierto programada en PHP y permite la instalación de nuevos componentes según las necesidades de los usuarios.

En la tabla 2 se presenta un cuadro comparativo entre 3 herramientas de administrador de contenidos y se especifican sus principales características.

Tabla 1. Comparativo entre modelos de desarrollo de software.

Modelo	Enfoque	Ventajas/Desventajas	Aplicabilidad
Cascada	El inicio de cada etapa debe esperar la finalización de la inmediatamente anterior.	Los proyectos rara vez siguen una evolución secuencial. No todos los requisitos son expuestos, al principio, de forma explícita como requiere este modelo.	Utilizado cuando existen especificaciones amplias de los requerimientos del cliente.
Basado en prototipos	Prototipos: No posee la funcionalidad total del sistema pero si condensa la idea principal del mismo, paso a paso crece su funcionalidad, alto grado de participación del usuario.	El cliente puede pensar que el prototipo es una versión acabada. Las herramientas elegidas pueden ser inadecuadas. La clave del éxito de este modelo consiste en definir bien, desde el principio, las reglas del juego. Alto grado de participación del usuario.	Para sistemas interactivos pequeños o de tamaño pequeño. Conveniente en caso de ser necesario desarrollar módulos.
Incremental o evolutivo	Modelo lineal-secuencial con el modelo basado en prototipos. El sistema no se entrega de una vez, si no que se divide y se entregan incrementos. Con cada incremento se entrega la parte de la funcionalidad que se ha establecido.	Los clientes no tienen que esperar hasta tener el sistema completo. Los primeros incrementos sirven como prototipo y ayudan en la tarea de detectar los posteriores requisitos. Existe un riesgo bajo de fallar en el proyecto total.	Reemplazar el antiguo desarrollo con uno nuevo que satisfaga las nuevas necesidades según las redefiniciones del problema. Manejo de versiones.
Modelo espiral.	Es una mejora del modelo basado en prototipos. Cada espiral representa una fase del proceso. Un ciclo a través de la espiral simula un paso a través de un modelo en cascada.	Requiere comunicación permanente con el cliente por lo tanto si se cambia el contacto con el cual se realiza desarrollo es necesario que esté al tanto de lo realizado y lo pendiente. El cliente debe ser gran conocedor del sistema.	Utilizado para el desarrollo de aplicaciones complejas o especificas.

Fuente: Sena regional Cauca. Junio 2009-2010. Disponible en: <http://www.slideshare.net.>

Tabla 2. Comparativo entre administradores de contenidos.

CARACTERÍSTICA	ENSITECH	GALEONPRO	MOODLE	JOOMLA
Espacio en Disco (MB)	4GB	4GB	2GB	23MB
Volumen de Transferencia (GB/mes)	10GB	40GB	40 GB	10GB
Sistema Operativo en el servidor	Windows, Linux	Linux	Unix, GNU/Linux, Open Solaris, FreeBSD, Windows, Mac OS X, NetWare	Windows, Linux
Panel de control personalizable	SI	SI	SI	SI
Estadísticas detalladas de visitas	SI	SI	SI	SI
Cuentas de correo	Limitadas	Limitadas	Ilimitadas	Ilimitadas
Lenguaje soportado PHP, PERL, FLASH	Limitados	SI	SI	SI
Acceso a Bases de Datos MYSQL	Limitadas	Limitadas	SI	SI
PhpMyAdmin	SI	SI	SI	SI
Precio Comercial Anual	$ 8.000.000 - $10.950.000	$10.463.120	US.700	Software Libre

Para la implementación del OVA es necesario establecer un estándar que permita la comunicación entre objetos pedagógicos y usuarios. La plataforma educativa tiene como fin la organización de pequeños conjuntos estructurados de objetos para ser publicados en un servidor web y de esta manera se pueda acceder a la información, utilizando internet.

SCORM es un estándar que cumple con servicios basados en web y permite la utilización de metadatos para que el OVA describa el contenido de recursos, por medio de un conjunto estructurado de elementos. Este estándar admite la publicación de contenidos pedagógicos para su reutilización.

Los requerimientos de SCORM para el Objeto virtual de aprendizaje son:

- **Interoperabilidad**: la plataforma exhibe y administra contenidos educativos, para ser implementados en otras plataformas y ser un material independiente de las herramientas utilizadas.

- **Reusabilidad**: el OVA se enfoca en la reutilización de contenidos, para aumentar la calidad de la información.

- **Manejabilidad**: por medio del panel de administración del OVA, es posible determinar la cantidad de usuarios registrados en el aplicativo. Consultando la base de datos se puede visualizar la fecha de la última visita de cada usuario, y su interacción con los contenidos.

- **Accesibilidad**: la plataforma estará disponible en un servidor web para que los usuarios con acceso a internet, puedan consultar los materiales educativos cuando lo requieran.

- **Durabilidad**: independientemente de los recursos tecnológicos que se utilicen para acceder a la plataforma, la estructura del OVA está diseñada para adaptarse y proveer funcionalidad.

- **Escalabilidad**: el objeto virtual permite adaptar nuevas funciones para interactuar con los usuarios. Es posible la publicación de más contenidos e incrementar el registro de usuarios.

- **Efectividad en los costos**: la publicación del OVA permite la visualización y reutilización de contenidos educativos para evitar el desplazamiento a las aulas físicas, lo que reduce costos para el usuario.

Los metadatos son información descriptiva acerca de un objeto o recurso. La metadata de Scorm se centra en el estándar IEEE 1484.12.1-2002 LTSC Learning Object Meta-data (LOM)[13] y ha sido divida en las siguientes categorías:

- **Categoría General:** presenta y describe el objeto.

- **Categoría del Ciclo de vida**: Se muestra la versión, estado, la historia y el estado actual del objeto.

- **Categoría de Meta-metadata**: describe información sobre la propia meta instancia.

- **Categoría Técnica**: esta parte presenta las características técnicas del objeto.

- **Categoría Educacional**: permite identificar las características pedagógicas del objeto de aprendizaje.

- **Categoría del Derecho**: se especifican condiciones de uso.

- **Categoría de Relación**: define la relación entre varios objetos.

- **Categoría de Anotaciones**: esta categoría presenta información sobre el uso educativo del OVA.

[13] LUCIANO, Denise. Noviembre de 2010. Meta-Objetos SCORM. [En linea]. [Consulta: Octubre 13 de 2010]. Disponible en: <http://xata.fe.up.pt/2006/papers/14.pdf>

4.2 MARCO LEGAL O NORMATIVO

En Colombia existen una serie de normas las cuales buscan proteger los sistemas de información. La problemática actual que se presenta en la seguridad de redes informáticas, estipula que es necesario guiarse por unas leyes establecidas por el ministerio de comunicación del estado colombiano.

En este marco normativo se presentan las acciones legales, decretos y sanciones que establece la ley, sobre la protección de la información por medio de acceso a Internet en Colombia. (Ver anexo B).

5. DESARROLLO INGENIERIL

5.1 METODOLOGÍA DEL PROYECTO

Una metodología es un esquema de trabajo que permite estructurar, planificar y controlar el proceso de desarrollo de software. Por medio de una metodología se establecen las etapas que tendrá el proyecto para elaborar de forma ordenada y funcional cada ítem del software.

El enfoque de la metodología es el modelo en cascada. Un modelo en cascada considera las principales actividades de especificación, desarrollo, validación y evolución del software y las divide en fases separadas. Las principales fases del modelo en cascada son:

- **Análisis y definición de requerimientos:** esta etapa del modelo, permite identificar la funcionalidad del software mediante las especificaciones de los usuarios. El análisis es la estructura para la elaboración de cualquier tipo de software que adopte este modelo.
- **Diseño**: permite establecer una arquitectura completa del sistema. El diseño identifica y describe las abstracciones fundamentales del software.
- **Implementación:** el diseño del software es desarrollado mediante un conjunto de actividades y posteriormente implementadas para su funcionamiento.
- **Pruebas:** permite la realización de pruebas para verificar el óptimo funcionamiento de los componentes del software.

5.2 ANÁLISIS DE REQUERIMIENTOS

Esta etapa del modelo, especifica los requerimientos funcionales y no funcionales para el desarrollo del simulador de seguridad en redes inalámbricas Wi-Fi. El aplicativo será un módulo del OVA que permite la configuración de las principales características de seguridad.

A continuación se explican las herramientas de aprendizaje que integran el Objeto Virtual, para promover el conocimiento entre docentes y estudiantes de la universidad de San Buenaventura (Bogotá).

- **Contenido:** en esta sección los administradores y docentes publican los temas que a su parecer cumplan con los niveles de enseñanza sobre la seguridad en redes inalámbricas Wi- Fi.

- **Noticias:** este módulo permite la publicación de noticias referente a la protección de los datos. Los administradores y docentes pueden determinar que artículos son importantes para informar a la comunidad educativa.

- **Enviar artículo:** por medio de un editor de texto, se da la opción de que los usuarios registrados en el OVA, puedan redactar sus propios artículos para su futura publicación.

- **Enviar enlace:** esta herramienta permite compartir links provenientes de internet. Es necesario conocer exactamente la URL de la pagina web para establecer la comunicación.

- **Zona de archivos:** esta sección permite a los docentes crear diferentes categorías para la descarga de archivos. En esta zona se pueden declarar las actividades y herramientas necesarias para la compresión de contenidos.

- **Foros:** este módulo establece la interacción entre los usuarios registrado del OVA. En esta parte se pueden publicar comentarios, ideas y sugerencias en las diferentes categorías creadas por administradores y docentes.

- **Eventos:** en esta parte se pueden publicar las diferentes actividades educativas que ofrezca la Universidad de San Buenaventura (Bogotá). Unos ejemplos de actividades pueden ser conferencias, cursos, talleres entre otros.

- **Mensajes:** es posible el envió de correos electrónicos entre usuarios. Esta herramienta es útil para la comunicación entre docentes y estudiantes.

5.2.1 Requerimientos Funcionales: a continuación se especifican los requerimientos funcionales del aplicativo “Simulador de seguridad Wi-Fi”:

- Autenticación para descargar el simulador de seguridad Wi-Fi.
- Selección de diversos dispositivos de red como portátiles, desktops, palms, y puntos de acceso.
- Ayuda desde el Objeto Virtual de Aprendizaje, para determinar las principales características de seguridad en cada dispositivo.
- Simulación de ondas en puntos de acceso.
- Detección automática de redes disponibles por parte de componentes de red (portátiles, desktops).
- Configuración de contraseñas en puntos de acceso para establecer conexiones.
- Elección del nombre de red (SSID), para identificar las redes.
- Selección de tipo de cifrado WPA o WEP.
- Validación de contraseñas entre puntos de acceso y dispositivos que deseen conectarse a una red determinada.
- Detección entre dispositivos de red y dispositivos cliente.
- Guardar redes o componentes de red por medio de archivos.

5.2.2 Requerimientos no funcionales: a continuación se especifican los requerimientos no funcionales del aplicativo “Simulador de Seguridad Wi-Fi”.

- El módulo del simulador de redes Wi-Fi, maneja la persistencia de información mediante archivos, no se utilizarán motores de bases de datos. Sin embargo el administrador de contenidos maneja una base de datos creada en MySQL.

- El almacenamiento de información está limitado a la capacidad del servidor donde este alojado el aplicativo.

- La disponibilidad del aplicativo depende del hosting en que se aloje.

- El tiempo de respuesta para el envío de archivos entre el cliente y servidor depende del tamaño del archivo y del ancho de banda con que se trabaje.

- El software es multiplataforma por estar desarrollado con código abierto en Java y html estándar. Funciona en un servidor con cualquier sistema operativo y desde cualquier navegador de internet.

- El rendimiento del aplicativo depende de las características de hardware y software del equipo donde se ejecute.

- La asignación de direcciones IP estáticas forman parte de información del aplicativo y no pueden ser configuradas.

5.2.3 Actores: en el desarrollo del Objeto virtual de Aprendizaje se encuentran 3 actores que son los encargados de interactuar con el sistema y el módulo del simulador de seguridad Wi-Fi. Estos actores se muestran en la Tabla 3.

Tabla 3. Descripción de Actores

Actores	Descripción
Administrador	Se encarga de configuraciones globales del administrador de contenidos Joomla y permite la gestión de archivos que se publiquen en la aplicación. Además utiliza el simulador de seguridad en redes Wi-Fi (ver Figura 2).
Docente	Este tipo de usuario se encarga del manejo de información que se presenta en el administrador de contenidos (Joomla). Tiene permisos para la utilización del simulador para seguridad de redes Wi-fi (ver Figura 3).
Estudiante	Es el encargado de interactuar con los contenidos publicados en Joomla. Tiene acceso al simulador de seguridad de redes Wi-Fi para la integración de conocimientos (ver Figura 4).

5.2.4 Casos de Uso: los casos de uso proporcionan una visión global sobre los requerimientos funcionales del sistema, para determinar el comportamiento del aplicativo. (Ver figura 2,3,4).

Figura 2. Casos de Uso del Administrador.

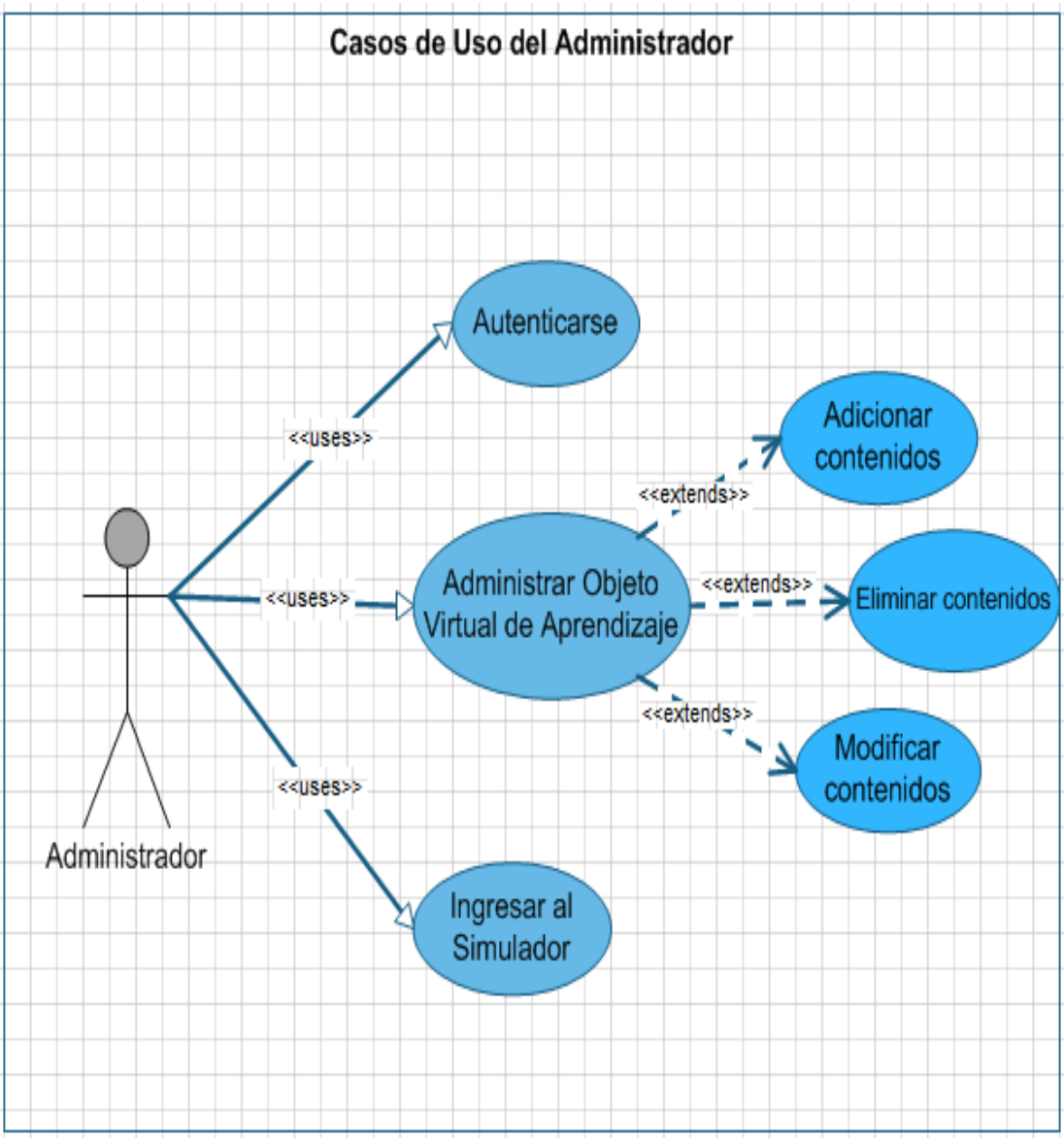


Figura 3. Caso de Uso del Docente.

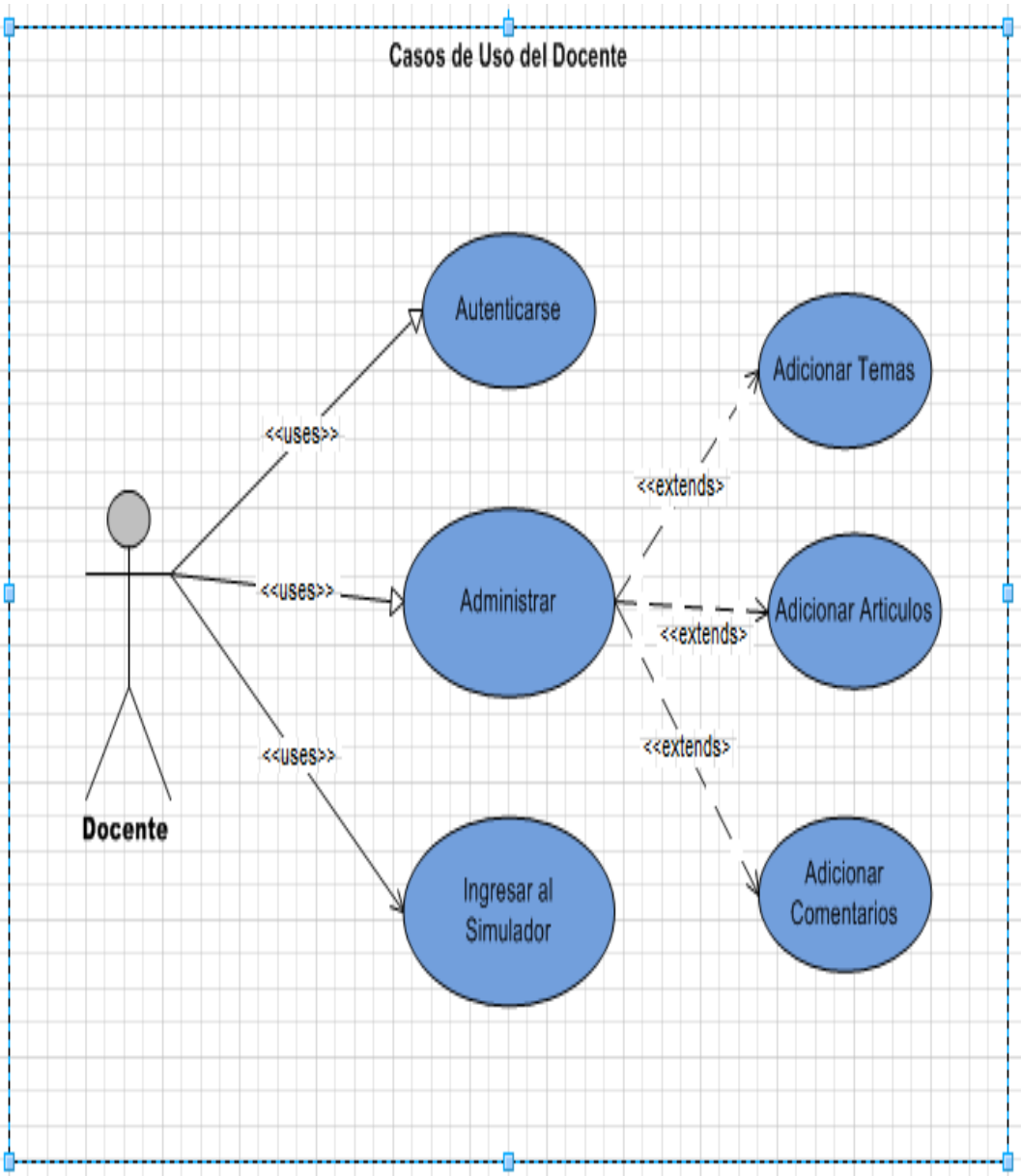
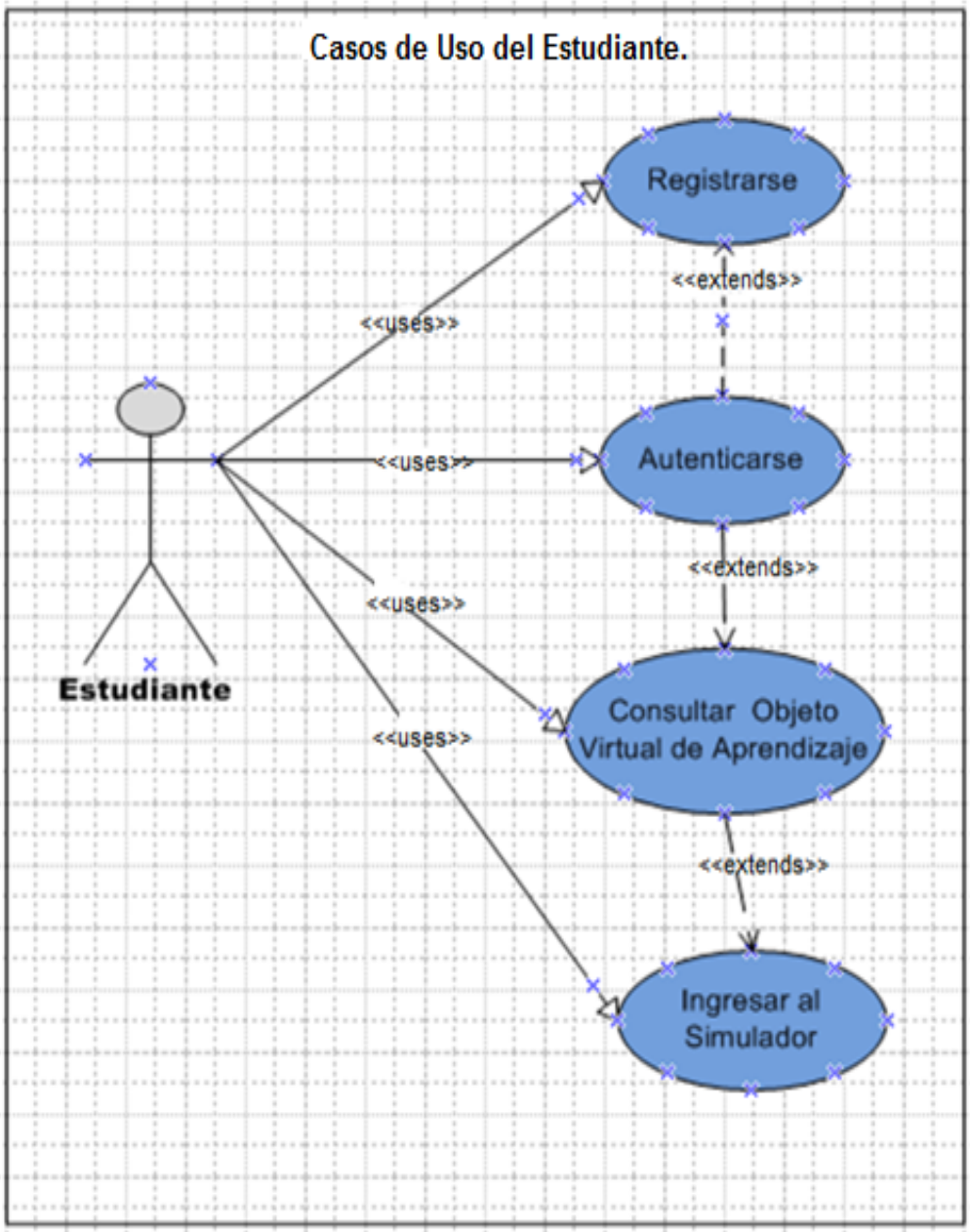


Figura 4. Caso de Uso del Estudiante.



5.2.5 Formatos y Diagramas de Casos de Uso: un diagrama de Casos de Uso es una representación gráfica que integra a los actores y casos de uso del sistema, en los cuales se incluyen sus interacciones.

Es necesario que cada caso de uso tenga un formato en el que se especifiquen objetivos, actores, curso normal de eventos, precondiciones, flujo alternativo de eventos y Pos condiciones. A continuación se presentan los casos de uso que intervienen en el sistema.

Figura 5. Diagramas de caso de uso Administrador

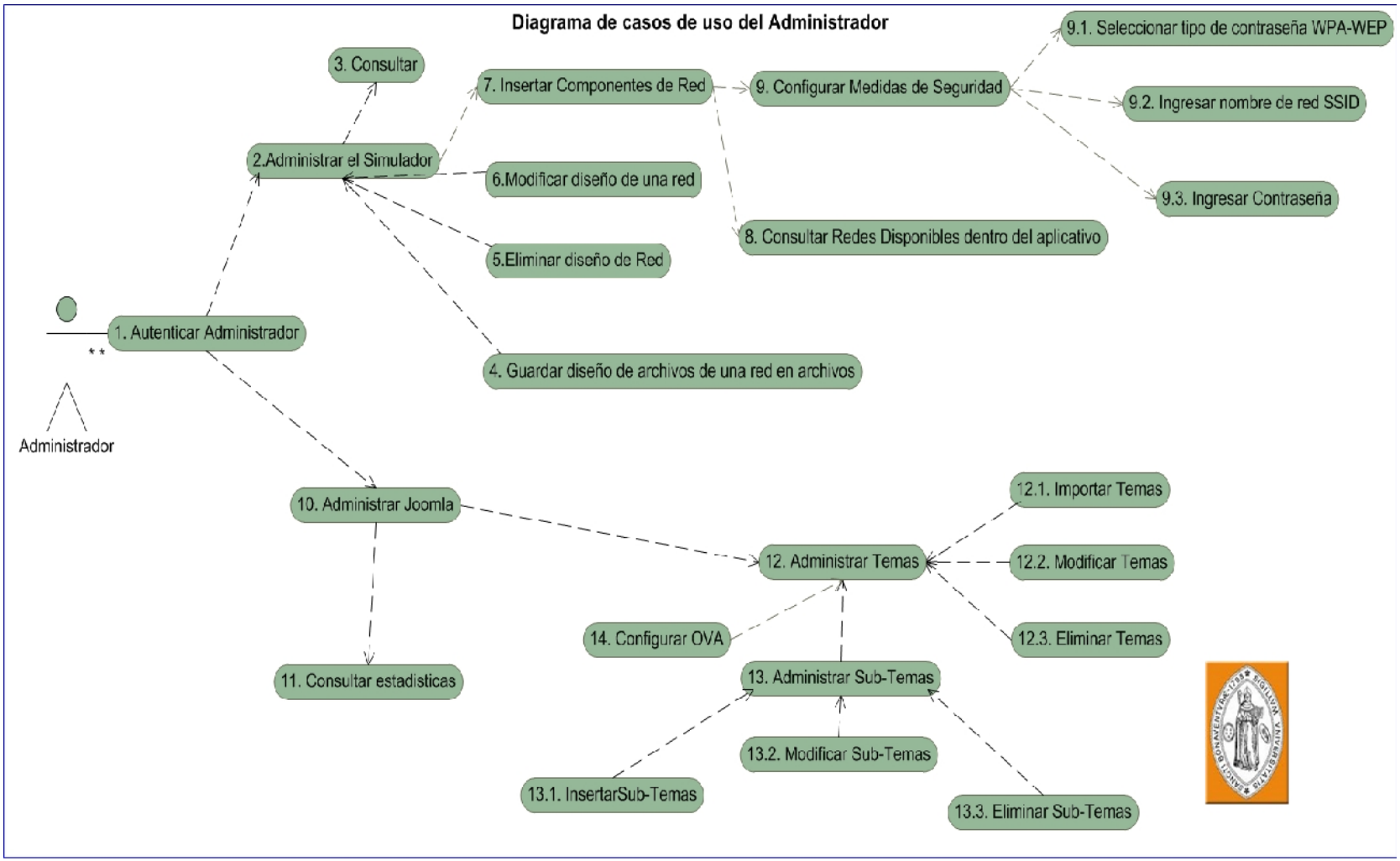


Tabla 4. Casos de uso Administrador Autenticar Usuarios

Caso de uso	**Autenticar Usuarios**	**Código: casos de uso 1 admin**
Objetivo	Validar usuario y contraseña del Administrador, Estudiante y Docente.	
Actores	Administrador, Estudiante, Docente	
Curso normal de eventos	1. El Administrador ingresa su usuario y contraseña. 2. Los datos son enviados al servidor.	
Precondiciones	Los usuarios deben existir en la base de datos de Joomla.	
Flujo alternativo de eventos	3. La contraseña o Usuario no es válida, el servidor debe informar al usuario que los datos no son validos.	
Pos condiciones	Usuario autenticado en el sistema.	

Tabla 5. Casos de uso Administrador Administrar el simulador

Caso de uso	**Administrar el simulador**	**Código: casos de uso 2 admin.**
Objetivo	Administrar el simulador de redes Wi-Fi.	
Actores	1 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. Diseñar una red Wi-fi adaptando medidas de seguridad disponible.	
Precondiciones	Los usuarios pueden diseñar un esquema de red inalámbrico Wi-Fi.	
Flujo alternativo de eventos	2. La documentación de ayuda esta publicada en Joomla para el desarrollo de la red inalámbrica.	
Pos condiciones	Los usuarios diseñan una red Wi-Fi.	

Tabla 6. Casos de uso Administrador Consultar

Caso de uso	**Consultar**	**Código: casos de uso 3 admin.**
Objetivo	Consultar dentro del OVA la documentación referente al uso del simulador.	
Actores	2 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. Genera dispositivos de red para implementarlos en el simulador.	
Precondiciones	Ayuda a los usuarios a manejar el simulador de redes Wi-Fi	
Flujo alternativo de eventos	2. Consultar la documentación y aplicar configuraciones en la red simulada.	
Pos condiciones	Generar consultas en el OVA para aplicar seguridad en la red simulada.	

Tabla 7. Casos de uso Administrador Guardar diseño de una red en archivos

Caso de uso	**Guardar diseño de una red en archivos**	**Código: casos de uso 4 admin.**
Objetivo	Guardar el diseño de una red Wi-Fi.	
Actores	2 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. Guardar la red cuando este diseñada o los cambios hechos en el área de trabajo del simulador.	
Precondiciones	Guarda la red diseñada por el usuario.	
Flujo alternativo de eventos	2. Guarda la red que está en diseño.	
Pos condiciones	El usuario guarda la red simulada mediante archivos.	

Tabla 8. Casos de uso Administrador Eliminar diseño de red

Caso de uso	**Eliminar diseño de red**	**Código: casos de uso 5 admin.**
Objetivo	Eliminar un diseño de red implementado anteriormente.	
Actores	2 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. Elimina los diseños de red, que el usuario seleccione.	
Precondiciones	Elimina archivos que hayan sido guardados con anterioridad.	
Flujo alternativo de eventos	2. Elimina por completo la red diseñada.	
Pos condiciones	Eliminar archivos guardados por el simulador.	

Tabla 9. Casos de uso Administrador Modificar diseño de una red

Caso de uso	**Modificar diseño de una red**	**Código: casos de uso 6 admin.**
Objetivo	Modificar una red guardada.	
Actores	2 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. Modificar una red diseñada con anterioridad.	
Precondiciones	Modificar el diseño de la red guardada anteriormente por el usuario	
Flujo alternativo de eventos	2. Modifica y muestra opciones para guardar los cambios efectuados en la nueva red.	
Pos condiciones	Modificar las simulaciones de red.	

Tabla 10. Casos de uso Administrador Insertar componentes de red

Caso de uso	Insertar componentes de red	Código: casos de uso 7 admin.
Objetivo	Insertar un componente al diseño de la red Wi-Fi	
Actores	2 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. Insertar PC dentro del simulador. 2. Insertar puntos de acceso para las redes de simulación.	
Precondiciones	Ubicar componentes de red dentro del simulador .	
Flujo alternativo de eventos	3. Posibles ubicaciones dentro del simulador.	
Pos condiciones	El aplicativo inserta los componentes necesarios para cada red.	

Tabla 11. Casos de uso Administrador Consultar redes disponibles dentro del aplicativo

Caso de uso	Consultar redes disponibles dentro del aplicativo	Código: casos de uso 8 admin.
Objetivo	Simular redes inalámbricas en el área de trabajo del aplicativo.	
Actores	8 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. Detectar las redes que estén al alcance de los dispositivos aplicados en el simulador.	
Precondiciones	Generar la simulación de los puntos de acceso.	
Flujo alternativo de eventos	2. Consultar las redes disponibles, para la conexión de los dispositivos de red.	
Pos condiciones	El aplicativo simule la conexión de dispositivos de red.	

Tabla 12. Casos de uso Administrador Configurar medidas de seguridad

Caso de uso	**Configurar medidas de seguridad**	**Código: casos de uso 9 admin.**
Objetivo	Configurar los medios de seguridad que el aplicativo posea.	
Actores	8 admin. Administrador, Estudiante, Docente.	
Curso normal de eventos	1. Consultar posibles configuraciones dentro del simulador.	
Precondiciones	Consultar la documentación publicada en el OVA, para determinar los mecanismos de seguridad implementados a la red simulada.	
Flujo alternativo de eventos	2. Aplicar configuraciones de seguridad para proteger la red simulada.	
Pos condiciones	Configuración para proteger la red.	

Tabla 13. Casos de uso Administrador seleccionar de contraseña WPA-WEP

Caso de uso	**Seleccionar tipo de contraseña WPA-WEP**	**Código: casos de uso 9.1 admin.**
Objetivo	Implementar un tipo de contraseña para validar dispositivos en la red.	
Actores	9 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. La elección de claves WPA-WEP proporcionan un mecanismo de seguridad para el diseño de la red.	
Precondiciones	Configurar dispositivos de red.	
Flujo alternativo de eventos	2. El OVA tiene documentación sobre mecanismos de seguridad en redes Wi-Fi, para ser aplicada al simulador.	
Pos condiciones	El simulador adapta las configuraciones de los usuarios.	

Tabla 14. Casos de uso Administrador Ingresar nombre de red SSID

Caso de uso	**Ingresar nombre de red SSID**	**Código: casos de uso 9.2 admin.**
Objetivo	Seleccionar un nombre de red SSID, para reconocer las redes disponibles en el simulador.	
Actores	9 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. Ingresar nombre de red SSID.	
Precondiciones	Ingresar un nombre de red, para ser identificada por los dispositivos de red.	
Flujo alternativo de eventos	2. El OVA permite consultar documentación para determinar la elección de un nombre de red.	
Pos condiciones	Generar nombre SSID.	

Tabla 15. Casos de uso Administrador Ingresar Contraseña

Caso de uso	**Ingresar Contraseña**	**Código: casos de uso 9.3 admin.**
Objetivo	Ingresar contraseñas a los dispositivos para determinar la conexión a las redes disponibles.	
Actores	9 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. Digitar contraseñas a dispositivos de red.	
Precondiciones	Determinar una contraseña para validar los dispositivos que deseen conectarse a la red simulada.	
Flujo alternativo de eventos	2. El OVA permite consultar documentación referente a elección de contraseñas, para evitar accesos no autorizados a la red simulada.	
Pos condiciones	Los puntos de acceso implementados en el simulador, adaptan las contraseñas suministradas por los usuarios.	

Tabla 16. Casos de uso Administrador Administrar Joomla

Caso de uso	Administrar Joomla	Código: casos de uso 10 admin.
Objetivo	Administra y permite realizar configuraciones globales en el OVA.	
Actores	1 admin. Administrador	
Curso normal de eventos	1. Administra Joomla y maneja las tareas que brinda este aplicativo. 2. Puede implementar y modificar lo que este aplicativo tiene.	
Precondiciones	Permite la publicación de temas referentes a la seguridad en redes inalámbricas.	
Flujo alternativo de eventos	3. Administra todos los aplicativos de Joomla.	
Pos condiciones	Administra los servicios implementados en el OVA.	

Tabla 17. Casos de uso Administrador consultar Estadística

Caso de uso	Consultar Estadística	Código: casos de uso 11 admin.
Objetivo	Genera y consulta resultados obtenidos en encuestas, para determinar la funcionalidad del OVA.	
Actores	11 admin. Administrador, Estudiante, Docente	
Curso normal de eventos	1. Consulta e indaga sobre el funcionamiento del OVA.	
Precondiciones	Generar encuestas para determinar posibles fallas en el OVA.	
Flujo alternativo de eventos	2. Registrar la valoración hecha por usuarios para determinar la funcionalidad del OVA.	
Pos condiciones	Analizar los resultados obtenidos por las encuestas.	

Tabla 18. Casos de uso Administrador Administrar Temas

Caso de uso	Administrar Temas	Código: casos de uso 12 admin.
Objetivo	Administrar los temas registrados en el OVA.	
Actores	11 admin. Administrador	
Curso normal de eventos	1. Administrar los temas y maneja las tareas que brinda este aplicativo. 2. Implementar y modificar temas publicados en el OVA.	
Precondiciones	Tener documentación para la generación de nuevos temas.	
Flujo alternativo de eventos	3. Subir al servidor los temas a publicar.	
Pos condiciones	Generar una lista de temas relacionados con la seguridad en redes inalámbricas Wi-Fi.	

Tabla 19. Casos de uso Administrador Insertar Temas

Caso de uso	Insertar Temas	Código: casos de uso 12.1 admin.
Objetivo	Insertar documentos sobre seguridad de redes informáticas, respetando derechos de autor.	
Actores	13 admin. Administrador, Docente	
Curso normal de eventos	1. Anexar temas al OVA.	
Precondiciones	Analizar la información que se quiere publicar en el OVA.	
Flujo alternativo de eventos	2. Administrar los documentos insertados dentro de Joomla.	
Pos condiciones	Insertar y publicar los temas sobre seguridad en redes Wi-Fi.	

Tabla 20. Casos de uso Administrador Modificar Temas

Caso de uso	Modificar Temas	Código: casos de uso 12.2 admin.
Objetivo	Modificar los temas publicados en el OVA.	
Actores	13 admin. Administrador, Docente	
Curso normal de eventos	1. Modificar la documentación registrada en el OVA.	
Precondiciones	Analizar las modificaciones que se deseen hacer en los artículos registrados en el OVA.	
Flujo alternativo de eventos	2. Administrar y modificar la información publicada en el aplicativo.	
Pos condiciones	Generar las modificaciones hecha a la información, y guardar los cambios.	

Tabla 21. Casos de uso Administrador Eliminar Temas

Caso de uso	Eliminar Temas	Código: casos de uso 12.3 admin.
Objetivo	Elimina los documentos o lo que se desee dentro del administrador de contenidos.	
Actores	13 admin. Administrador	
Curso normal de eventos	1. Elimina los temas seleccionados.	
Precondiciones	Tener publicado en el OVA temas relacionados con la seguridad en redes inalámbricas.	
Flujo alternativo de eventos	2. Elimina la información contenida en el OVA.	
Pos condiciones	Seleccionar los temas que se desean eliminar y guardar los cambios.	

Tabla 22. Casos de uso Administrador Administrar Sub-Temas

Caso de uso	**Administra Sub-Temas**	**Código: casos de uso 13 admin.**
Objetivo	Administrar los sub-temas publicados en el OVA.	
Actores	13 admin. Administrador, Docente	
Curso normal de eventos	1. Administrar los sub-temas registrados por los docentes y administradores.	
Precondiciones	Evalúa la importancia de los Sub-temas que se quieren mostrar dentro de Joomla	
Flujo alternativo de eventos	2. Modifica y organiza todos los documentos puestos dentro del aplicativo.	
Pos condiciones	Administrar los subtemas.	

Tabla 23. Casos de uso Administrador Insertar Sub-Temas

Caso de uso	**Inserta Sub-Temas**	**Código: casos de uso 13.1 admin.**
Objetivo	Insertar documentos e información sobre seguridad en redes inalámbricas, respetando derechos de autor.	
Actores	14 admin. Administrador, Docente	
Curso normal de eventos	1. Insertar documentación para ser visualizada por los usuarios.	
Precondiciones	Evalúa la importancia de los sub-temas que se quieren mostrar dentro de Joomla	
Flujo alternativo de eventos	2. Registrar la documentación a publicar dentro del OVA.	
Pos condiciones	Registrar y publicar subtemas referentes a la seguridad en redes Wi-Fi.	

Tabla 24. Casos de uso Administrador Modificar Sub-Temas

Caso de uso	**Modificar Sub-Temas**	**Código: casos de uso 13.2 admin.**
Objetivo	Modificar subtemas publicados en el OVA.	
Actores	14 admin. Administrador, Docente	
Curso normal de eventos	1. Modificar los documentos que se deseen.	
Precondiciones	Analizar los sub-temas que se quieren publicar dentro de Joomla	
Flujo alternativo de eventos	2. Administra todos los documentos y modifica la información que lo requiera.	
Pos condiciones	Modificar los subtemas que se seleccionen y guarda los cambios.	

Tabla 25. Casos de uso Administrador Eliminar Sub-Temas

Caso de uso	**Eliminar Sub-Temas**	**Código: casos de uso 13.3 admin.**
Objetivo	Elimina los documentos o lo que desee dentro del administrador de contenidos.	
Actores	14 admin. Administrador	
Curso normal de eventos	1. Elimina los sub-temas registrados en el OVA.	
Precondiciones	Analizar los subtemas registrados en el OVA, para determinar qué información debe ser eliminada.	
Flujo alternativo de eventos	2. Elimina los documentos seleccionados.	
Pos condiciones	Elimina los subtemas seleccionados y guarda los cambios.	

Tabla 26. Casos de uso Administrador Configurar el OVA

Caso de uso	**Configurar el OVA**	**Código: casos de uso 14 admin.**
Objetivo	Consultar y modificar la configuración global del OVA.	
Actores	13 admin. Administrador	
Curso normal de eventos	1. Instalar, eliminar y administrar el aplicativo.	
Precondiciones	Administrar el aplicativo para realizar configuraciones globales.	
Flujo alternativo de eventos	2. Modificar el Objeto Virtual de Aprendizaje.	
Pos condiciones	Guardar la nueva configuración.	

Figura 6. Diagrama de Caso de Uso Docente

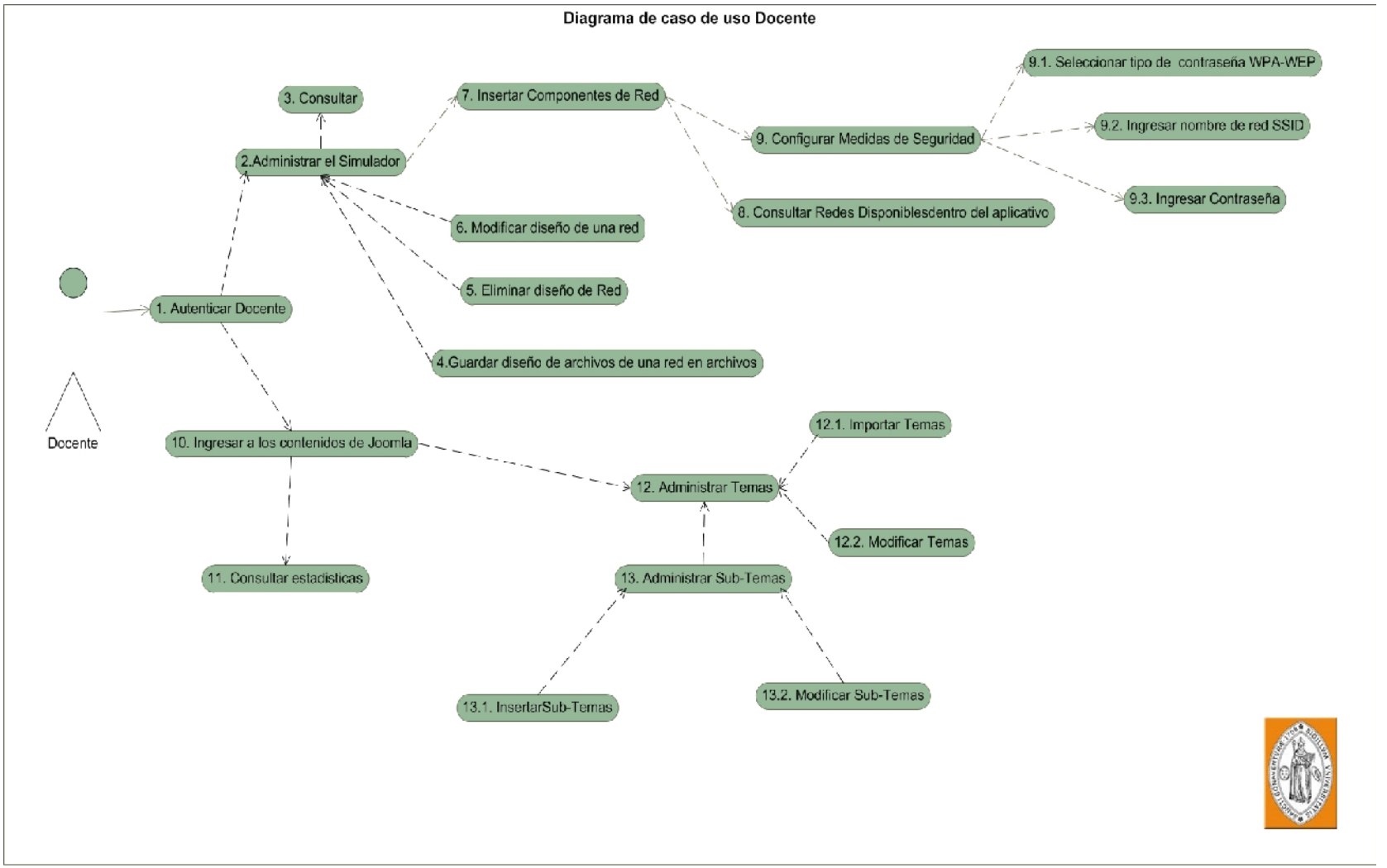


Tabla 27. Casos de uso Docente Ingresar a los Contenidos de Joomla

Caso de uso	**Ingresar a los contenidos de Joomla**	**Código: casos de uso 10 docente.**
Objetivo	Ingresar a los contenidos del aplicativo	
Actores	11 Docente.	
Curso normal de eventos	1. Ingresar al aplicativo y mantener los temas y sub temas actualizados	
Precondiciones	Ingresar al aplicativo y administrar temas y subtemas del OVA.	
Flujo alternativo de eventos	2. Mantener actualizado los materiales que desarrollan los estudiantes. 3. Publicar nuevos materiales educativos relacionados a la seguridad en redes inalámbricas.	
Pos condiciones	Mantener la información actualizada.	

Tabla 28. Casos de uso Docente Administrar Temas

Caso de uso	**Administrar Temas**	**Código: casos de uso 12 docente.**
Objetivo	Consultar el contenido que se quiere publicar y registrar documentos e información en el OVA.	
Actores	11 Docente.	
Curso normal de eventos	1. Publicar temas al aplicativo.	
Precondiciones	Consultar información sobre la seguridad en redes informáticas y analizar el contenido a publicar en el OVA.	
Flujo alternativo de eventos	2. Administrar el contenido publicado por el docente encargo para futuras publicaciones en el aplicativo.	
Pos condiciones	Mantener al usuario informado de las actividades y del material ingresado en el OVA.	

Tabla 29. Casos de uso Docente Administrar Sub-Temas

Caso de uso	**Administrar Sub-Temas**	**Código: casos de uso 13 docente.**
Objetivo	Diseñar herramientas virtuales para fomentar el uso de nuevas tecnologías educativas.	
Actores	13 Docente.	
Curso normal de eventos	1. Administrar subtemas publicados en el OVA.	
Precondiciones	Consultar información para ser publicada.	
Flujo alternativo de eventos	2. Administrar el contenido publicado en los subtemas para futuras publicaciones en el OVA.	
Pos condiciones	Publicar subtemas que permitan desarrollar nuevos conocimientos.	

Figura 7. Caso de Uso Estudiante.

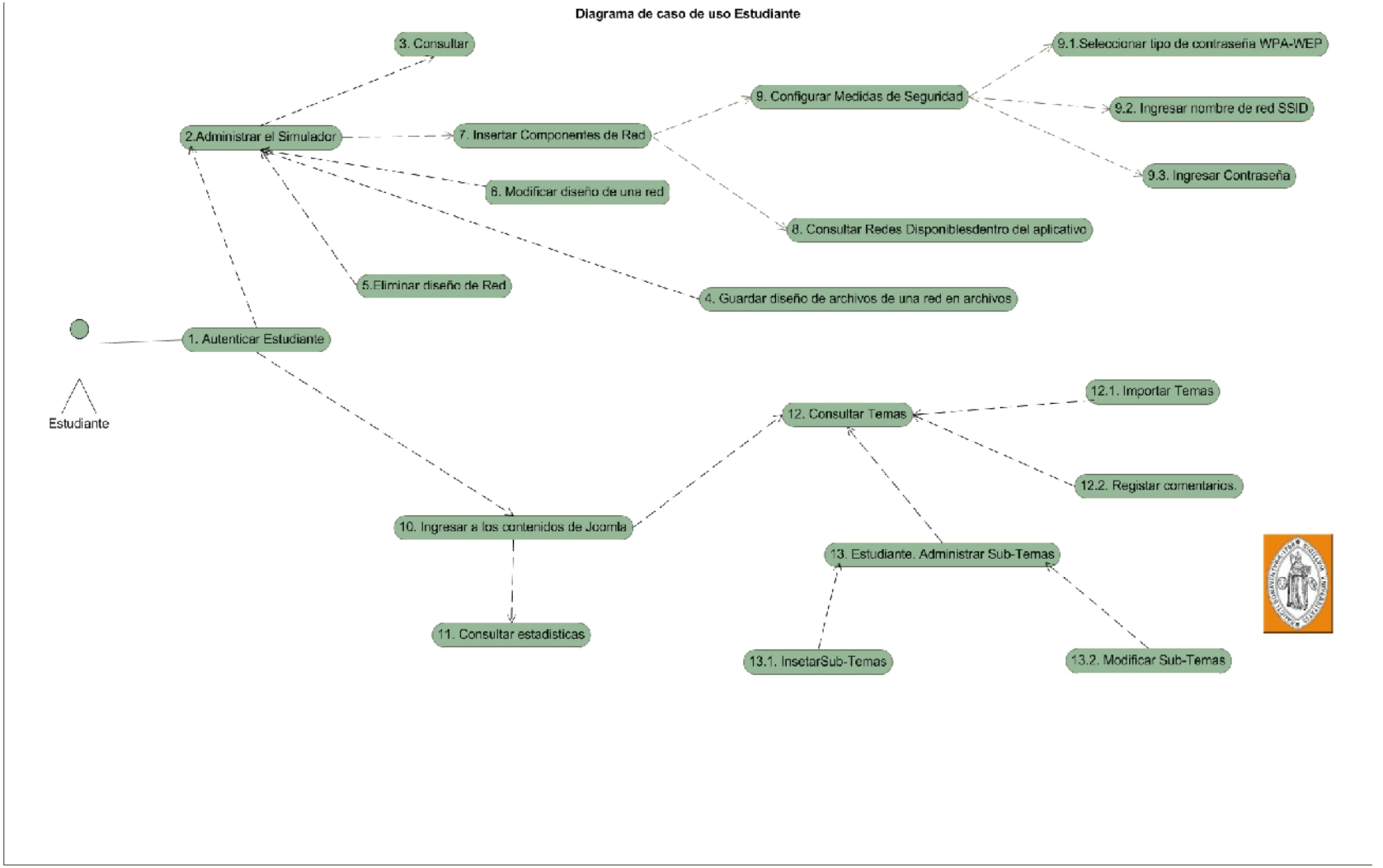


Tabla 30. Casos de uso Estudiante Ingresar a los Contenidos de Joomla

Caso de uso	**Ingresar a los contenidos de Joomla**	**Código: casos de uso 10 estudiantes.**
Objetivo	Ingresar a los contenidos del aplicativo	
Actores	Estudiante.	
Curso normal de eventos	1. Ingresar al aplicativo y poder visualizar la información publicada en el OVA.	
Precondiciones	Ingresar al aplicativo y consultar temas y subtemas publicados en el aplicativo.	
Flujo alternativo de eventos	2. Ingresar a los materiales desarrollados por otros usuarios y analizar la información.	
Pos condiciones	Publicar nueva documentación referente a la seguridad en redes inalámbrica, respetando derechos de autor.	

Tabla 31. Casos de uso Estudiante Consultar Temas

Caso de uso	**Consultar Temas**	**Código: casos de uso 12 estudiantes.**
Objetivo	Consultar la información y documentación publicada en el OVA.	
Actores	Estudiante.	
Curso normal de eventos	1. Descargar documentos e información publicados en el aplicativo, para su futuro análisis.	
Precondiciones	Autenticarse en el OVA.	
Flujo alternativo de eventos	2. Consultar los contenidos publicados en el OVA.	
Pos condiciones	Adquirir documentación sobre el diagnóstico y seguimiento de vulnerabilidades en redes Wi-Fi.	

Tabla 32. Casos de uso Estudiante Registrar comentarios

Caso de uso	Registrar comentarios.	Código: casos de uso 12.2 estudiantes.
Objetivo	Registrar comentarios referentes a la seguridad en redes Wi-Fi, para integrar los conocimientos entre usuarios.	
Actores	13 Estudiantes.	
Curso normal de eventos	1. Ingresar comentarios sobre temas publicados en el OVA..	
Precondiciones	Publicar comentarios en el OVA, para ser analizados por otros usuarios.	
Flujo alternativo de eventos	2. Registrar nuevos comentarios sobre la seguridad en redes Wi-Fi.	
Pos condiciones	Publicar información confiable, para ser consultada por los usuarios registrados en el OVA.	

Tabla 33. Casos de uso Estudiante Ingresar a los Contenidos de Joomla

Caso de uso	Consultar Sub-Temas	Código: casos de uso 14 estudiantes.
Objetivo	Diseñar nuevas formas de aprendizaje para los usuarios	
Actores	13 Estudiantes.	
Curso normal de eventos	1. Analizar subtemas publicados en el OVA.	
Precondiciones	Consultar la documentación registrada por los usuarios.	
Flujo alternativo de eventos	2. Descargar material educativo publicado en el OVA, para su futuro análisis.	
Pos condiciones	Publicar nueva documentación referente a la seguridad en redes inalámbrica, respetando derechos de autor.	

5.3 DISEÑO

El diseño del Objeto Virtual de Aprendizaje tiene como propósito crear una arquitectura para la futura implementación del proyecto. Por medio del siguiente diseño se establece la estructura estática y dinámica del aplicativo.

Para crear la estructura general del sistema se desarrollaron diversos tipos de diagramas que permiten modelar el aplicativo y definir la funcionalidad del mismo. Los diagramas que se utilizan en esta fase del proyecto son:

- Diagrama de Despliegue de componentes
- Mapa de navegación.
- Diagrama de secuencias.
- Diagrama de clases.

5.3.1 Diagrama de Despliegue de componentes: el diagrama de despliegue de componentes permite identificar los niveles y capas que intervienen en el aplicativo. El objetivo primordial de este tipo de diagramas para el Objeto Virtual de Aprendizaje, es dividir la lógica del negocio de la lógica del diseño.

En la siguiente figura se ilustra la separación de la capa de presentación, la capa de negocio y la capa de datos.

La capa de presentación permite que los usuarios que interactúan con el sistema se comuniquen con la capa del negocio, por medio de una interfaz grafica. Los actores que intervienen son administradores, docentes, estudiantes y usuarios externos. Esta capa captura la información de los usuarios y la procesa para establecer una comunicación.

La capa de negocio recibe las peticiones de los usuarios y ejecuta los procesos solicitados. Esta capa presenta lo siguiente:

- Autenticar usuario.
- Administrar OVA.
- Consulta Temas y Subtemas.
- Descarga simulador.

.

La capa de negocio se comunica con la capa de presentación para autenticar usuarios y presentar los contenidos de la plataforma. La lógica del negocio también se comunica con la capa de datos para solicitar al motor de la base de datos y archivos almacenar y consultar la información.

En la capa de negocio se descarga el simulador de seguridad de redes Wi-Fi y se administra dicha herramienta. El simulador presenta los siguientes procesos:

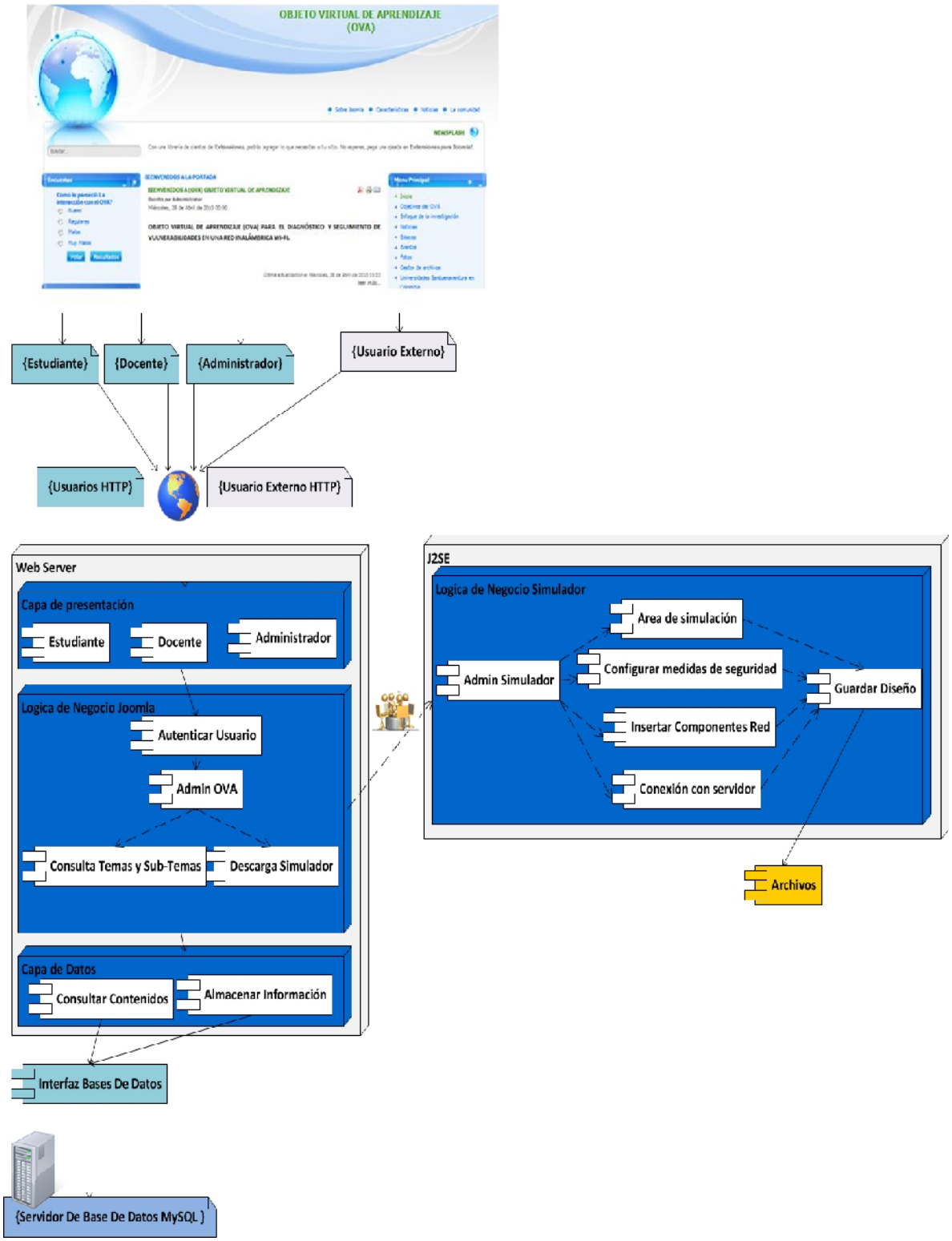
- Administrar simulador.
- Área de simulación.
- Insertar componentes de red.
- Configurar medidas de seguridad.
- Guardar diseño.

Por último se presenta la capa de datos en la cual se encuentra lo siguiente:

- Consultar contenidos.
- Almacenar información.

Esta capa se comunica con el servidor de base de datos Mysql, para recibir solicitudes de almacenamiento o consulta dependiendo la petición de la capa de negocio (ver figura 8).

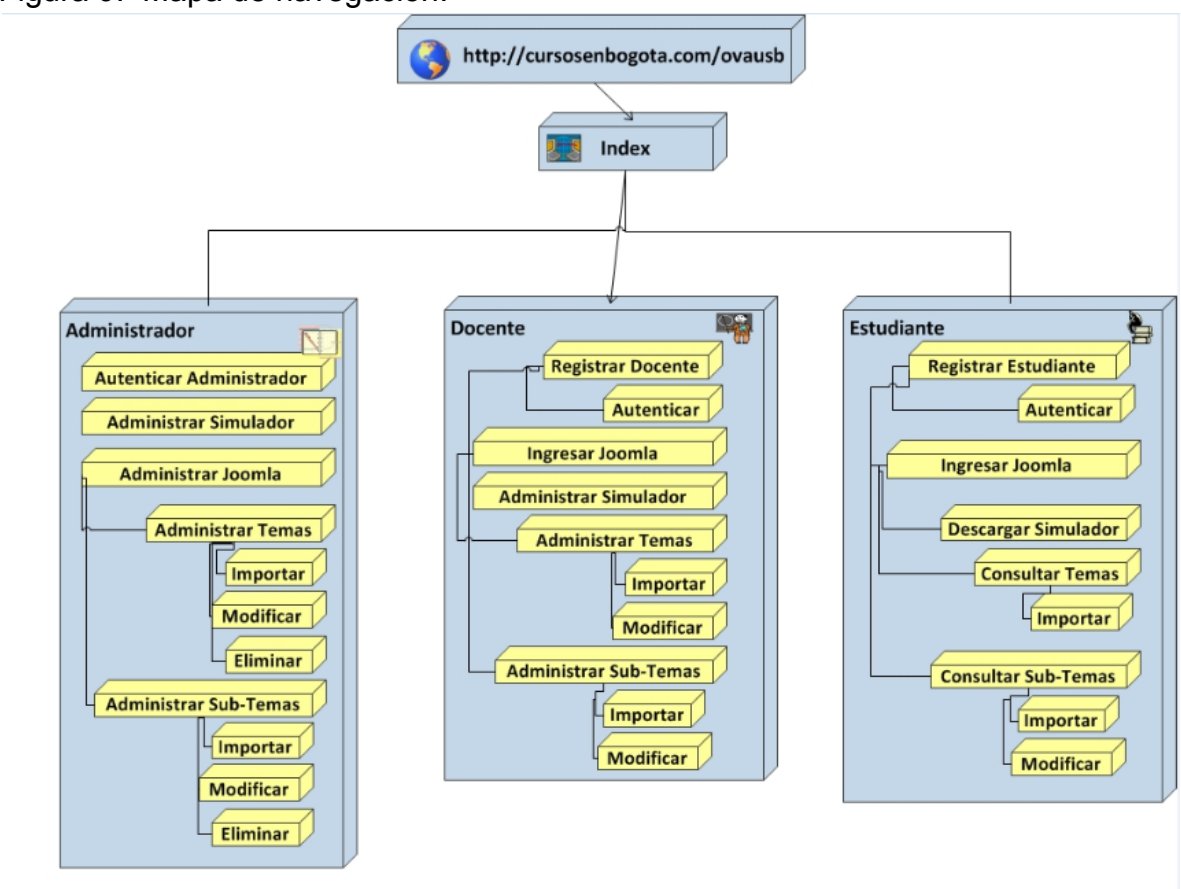
Figura 8. Diagrama de Despliegue de componentes.



5.3.2 Mapa de Navegación*:* en la figura 9 se observa la interacción de usuarios con la plataforma. El administrador se encarga de consultar o registrar a los docentes y estudiantes de la Universidad San Buenaventura. Otra función de un administrador es la configuración global del sistema.

El docente al igual que el estudiante tiene las opciones de ver los contenidos propuestos por el administrador o por otros docentes, pueden realizar ejercicios propuestos, actualizar algunos datos como son: Nombre, E-mail, contraseña Idioma, Zona Horaria, pero adicionalmente el docente puede ver los trabajos realizados por cada estudiante y acceder a la información de este.

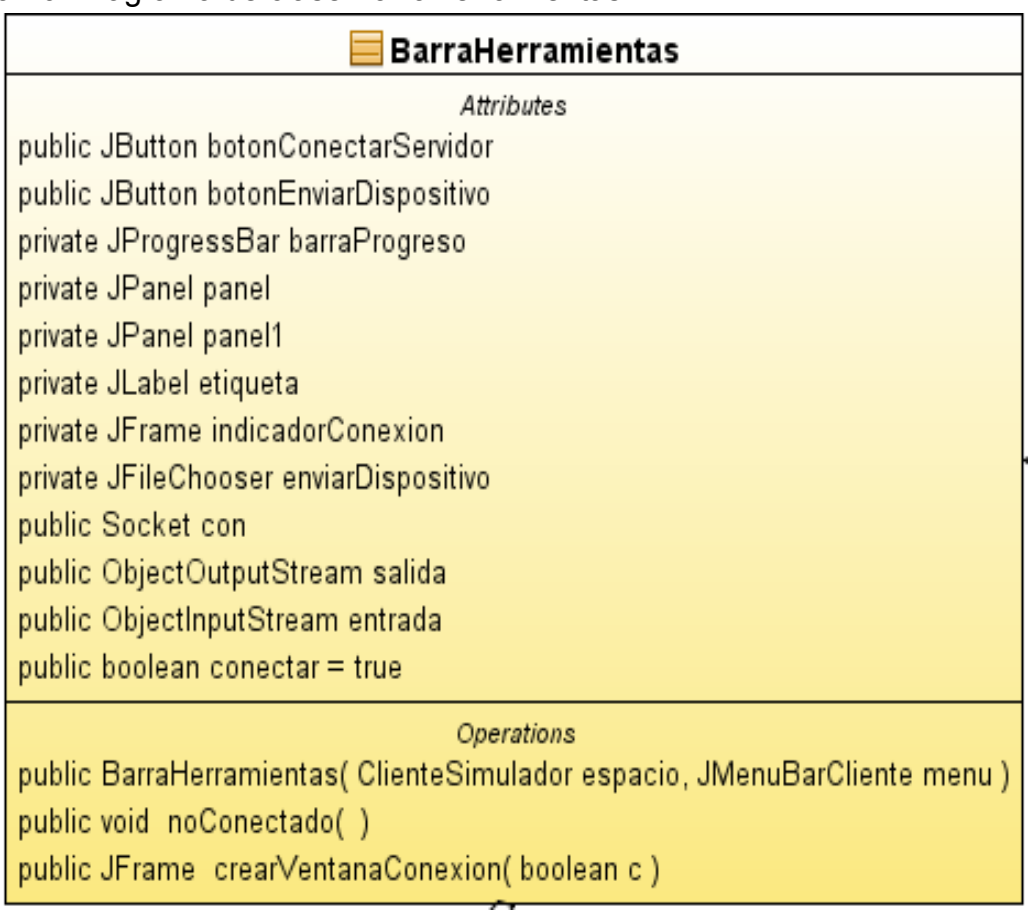
Figura 9. Mapa de navegación.



5.3.3 Diagramas de Clases: para determinar los atributos y comportamientos que tiene el modulo del simulador de seguridad en redes Wi-Fi, se realizaron diagramas de clases. Por medio de estos diagramas, se explican las características y objetos que representan la aplicación. A continuación se presentan cada una de las clases que intervienen en el software y por último se muestra un diagrama completo de clases con sus respectivas instancias (Ver figura 23).

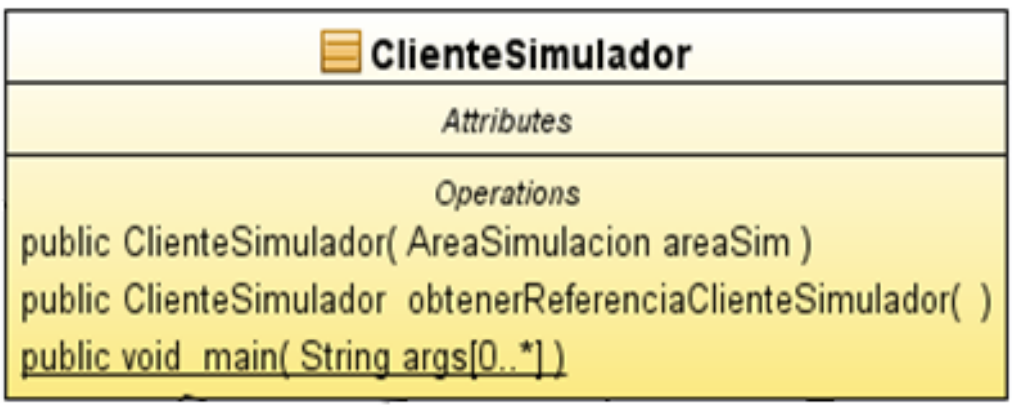
- **Diagrama de clase BarraHerramientas*:*** esta clase permite crear una barra de herramientas para la conexión con el servidor. Por medio de hilos o Threads se pueden establecer diversas conexiones para enviar y recibir dispositivos de red (Ver Figura 10)**.**

Figura 10. Diagrama de clase BarraHerramientas



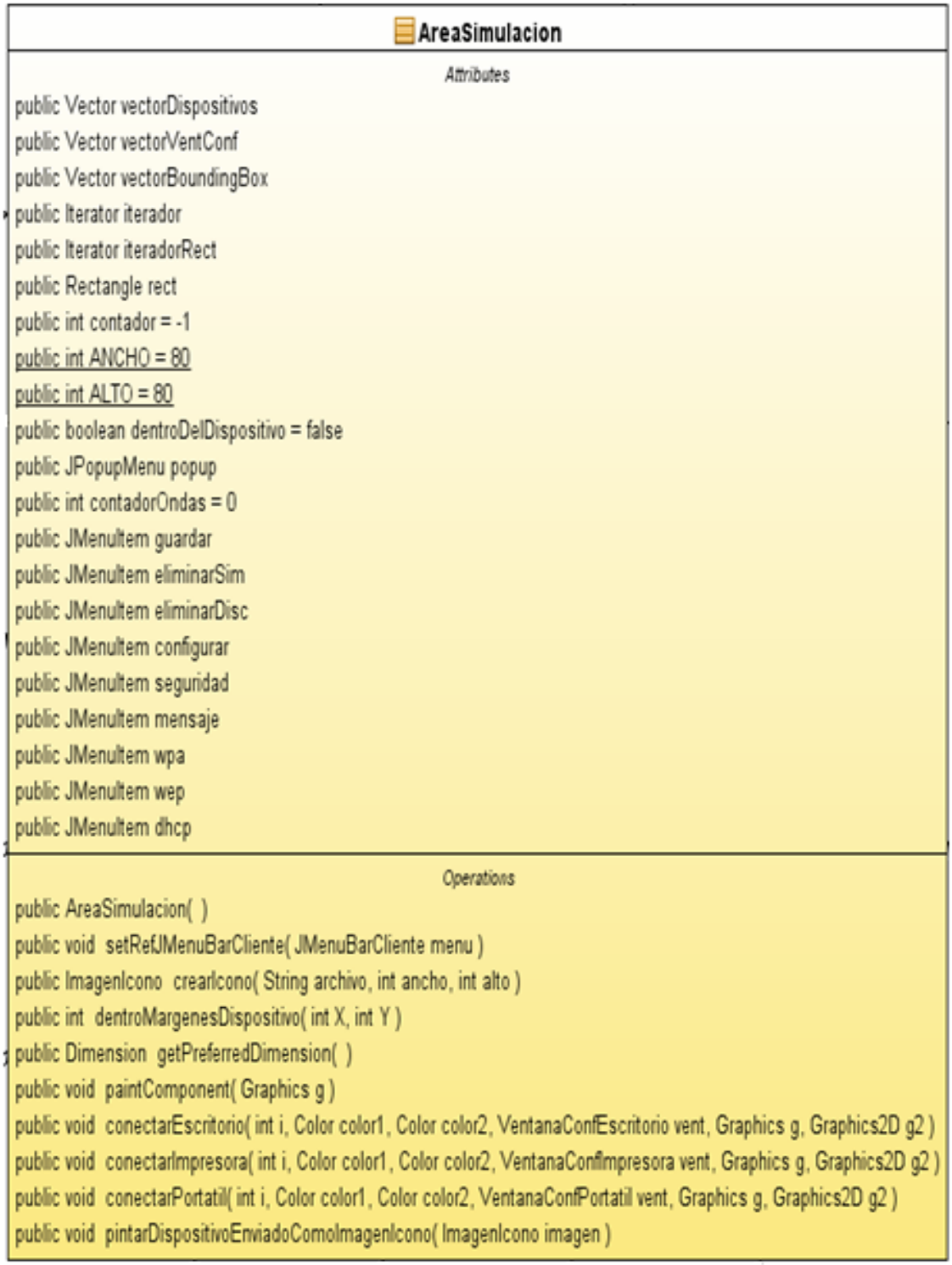
- **Diagrama de clase ClienteSimulador:** Esta es la clase principal. Esta clase se extiende de JFrame para crear una ventana u objeto Cliente Simulador en donde se establece el área de trabajo con menús, paneles y barras para la interacción con los usuarios (ver figura11).

Figura 11. Diagrama de clase ClienteSimulador



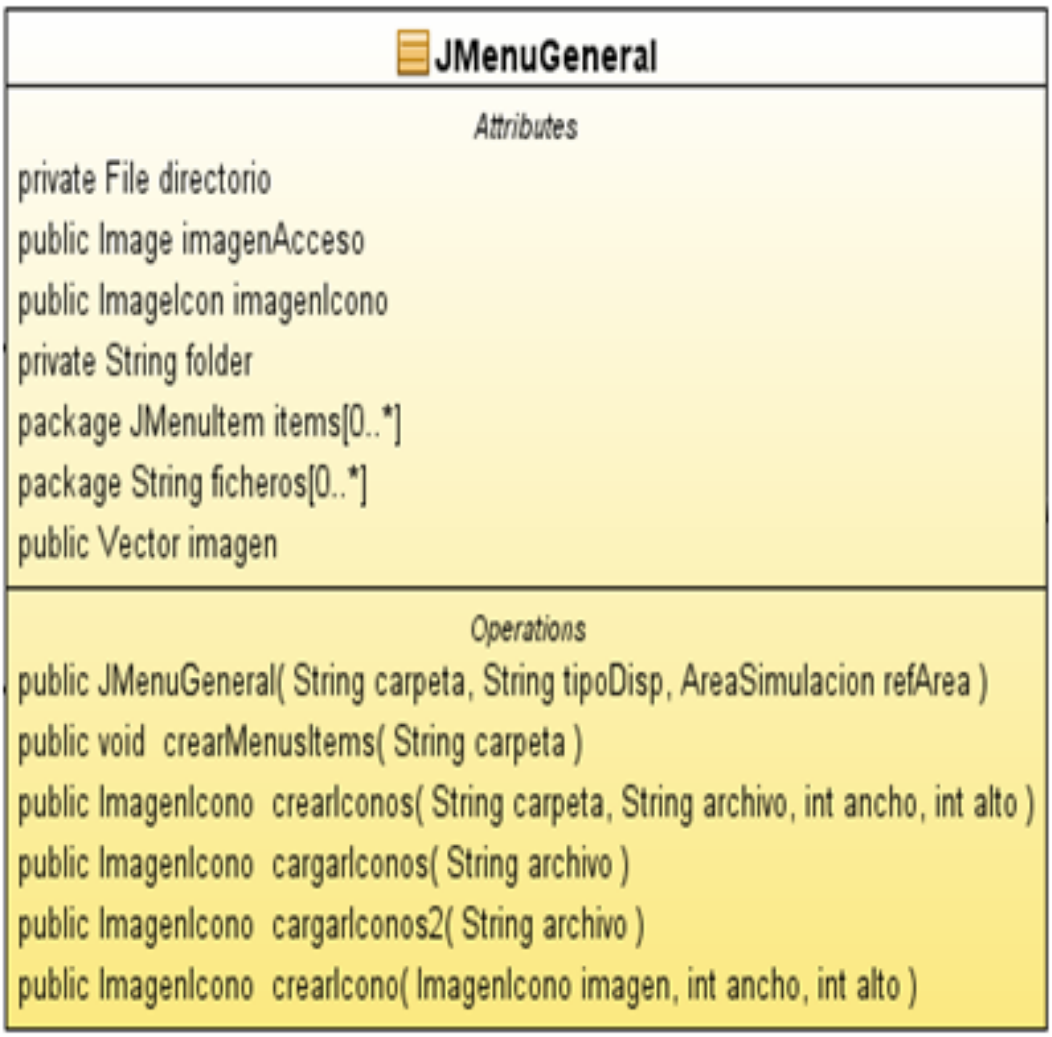
- **Diagrama de clase AreaSimulacion:** La clase AreaSimulacion extiende o hereda a JPanel, para crear la simulación de la red inalámbrica. Se utiliza el método paintcomponent para insertar las imágenes necesarias a la hora de implementar una red (ver figura 12).

Figura 12. Diagrama de clase AreaSimulacion.



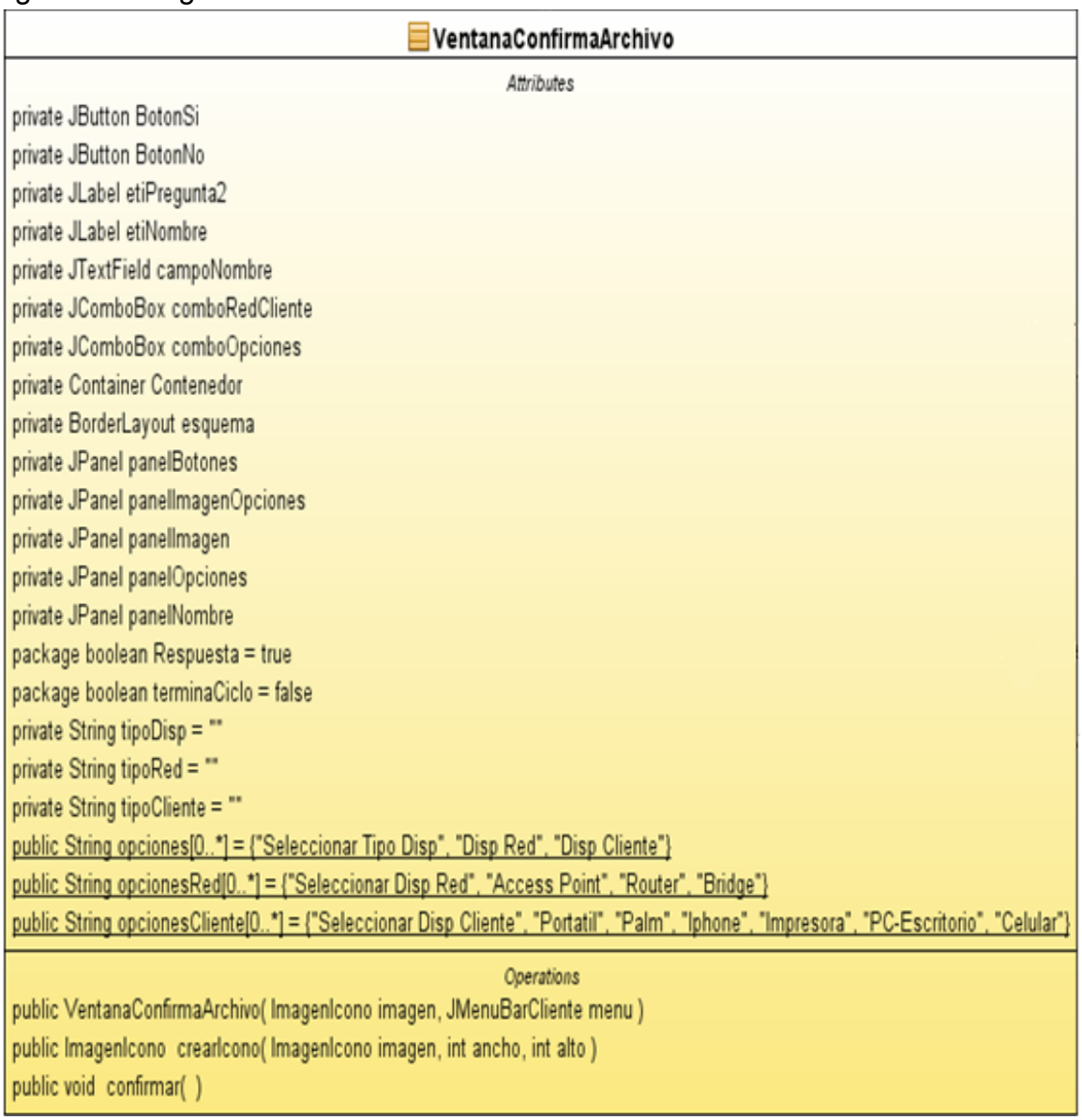
- **Diagrama de clase JMenuGeneral:** Esta clase JMenuGeneral es la encargada de crear los menús con sus respectivas opciones, iconos y nombres. Tiene un constructor JMenuGeneral que recibe dos parámetros. El primer parámetro se utiliza para localizar la carpeta de dispositivos y el segundo indica el conjunto de dispositivos que contendrá el menú ver (figura 13).

Figura 13. Diagrama de clase JMenuGeneral



- **Diagrama de clase VentanaConfirmaArchivo:** Esta clase le permite al usuario seleccionar un dispositivo de red, o un dispositivo cliente para ser implementado en el área de simulación. Un ejemplo de estos dispositivos es un access point (ver figura 14).

Figura 14. Diagrama de clase VentanaConfirmaArchivo

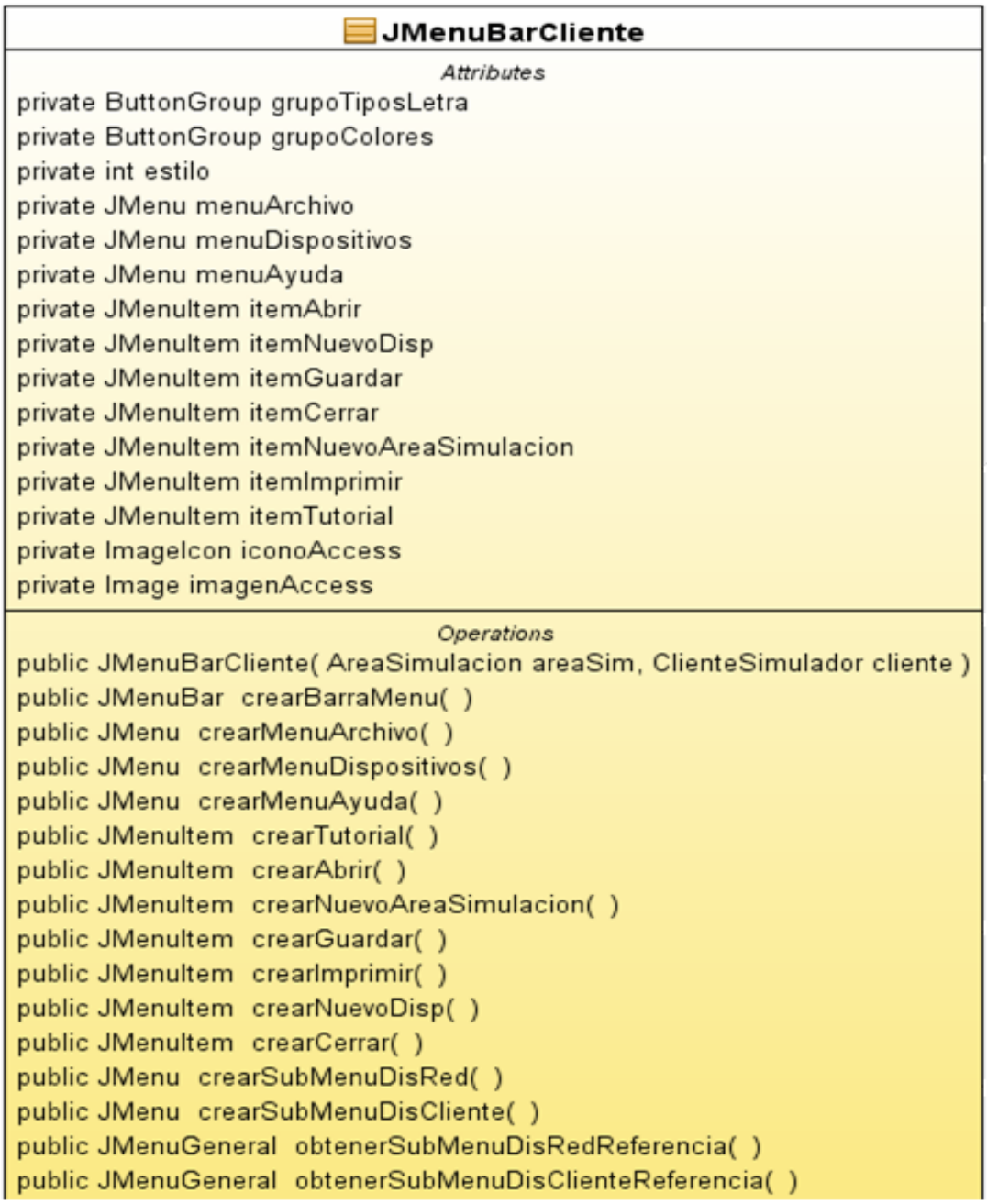


- **Diagrama de clase ImagenIcono:** Esta clase tiene como propósito crear imágenes cuando sea instanciada. El constructor ImagenIcono recibe un parámetro de tipo Image para ser tratada como ImageIcon. Se pueden establecer y obtener las coordenadas x, y para ser dibujada en JPanel (ver figura 15).

Figura 15. Diagrama de clase ImagenIcono

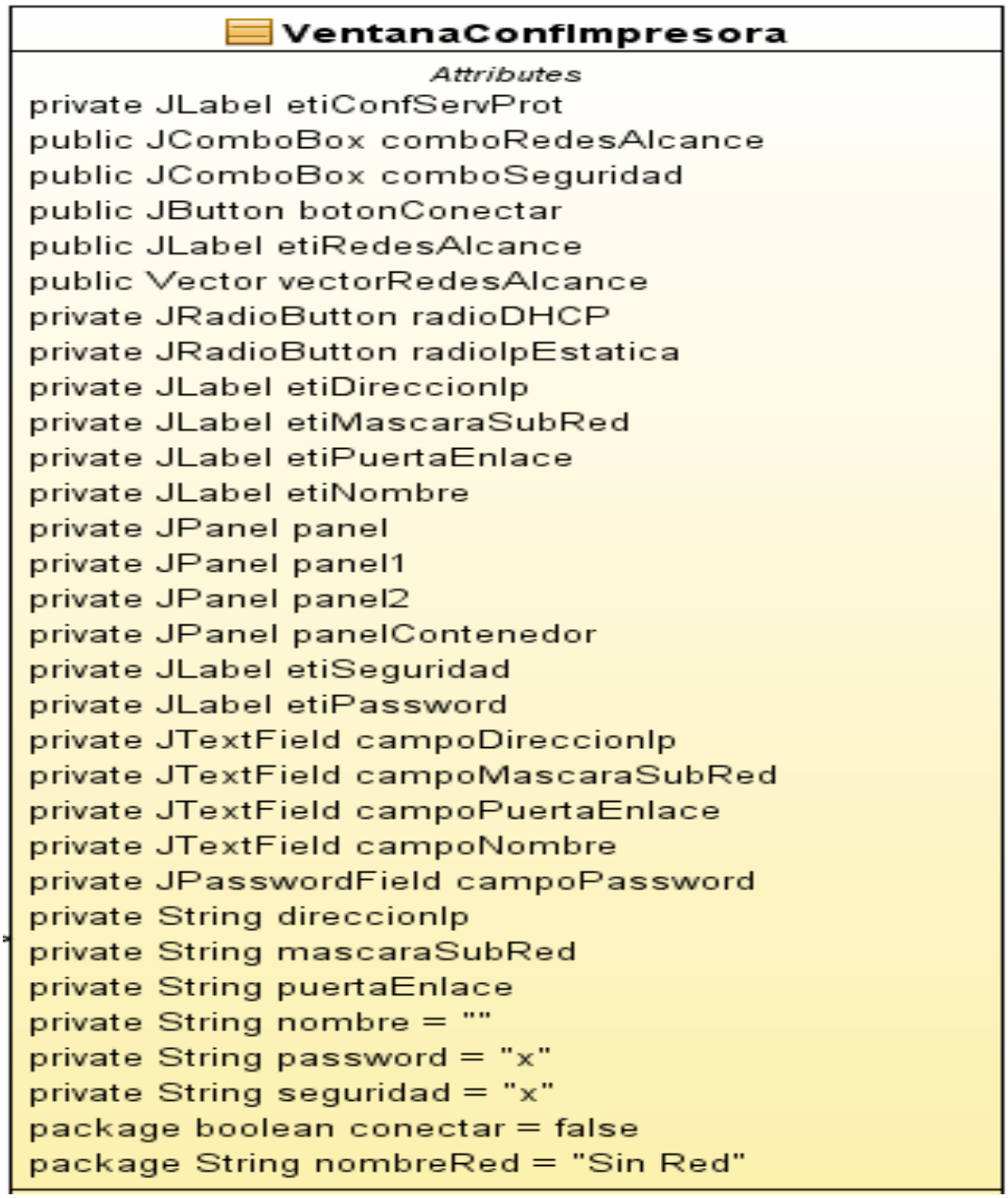
- **Diagrama de clase JMenuBarCliente:** Esta clase tiene por objeto crear una barra de menús y submenús para cargar imágenes y asignarles un titulo a cada opción seleccionada (ver figura 16).

Figura 16. Diagrama de clase JMenuBarCliente



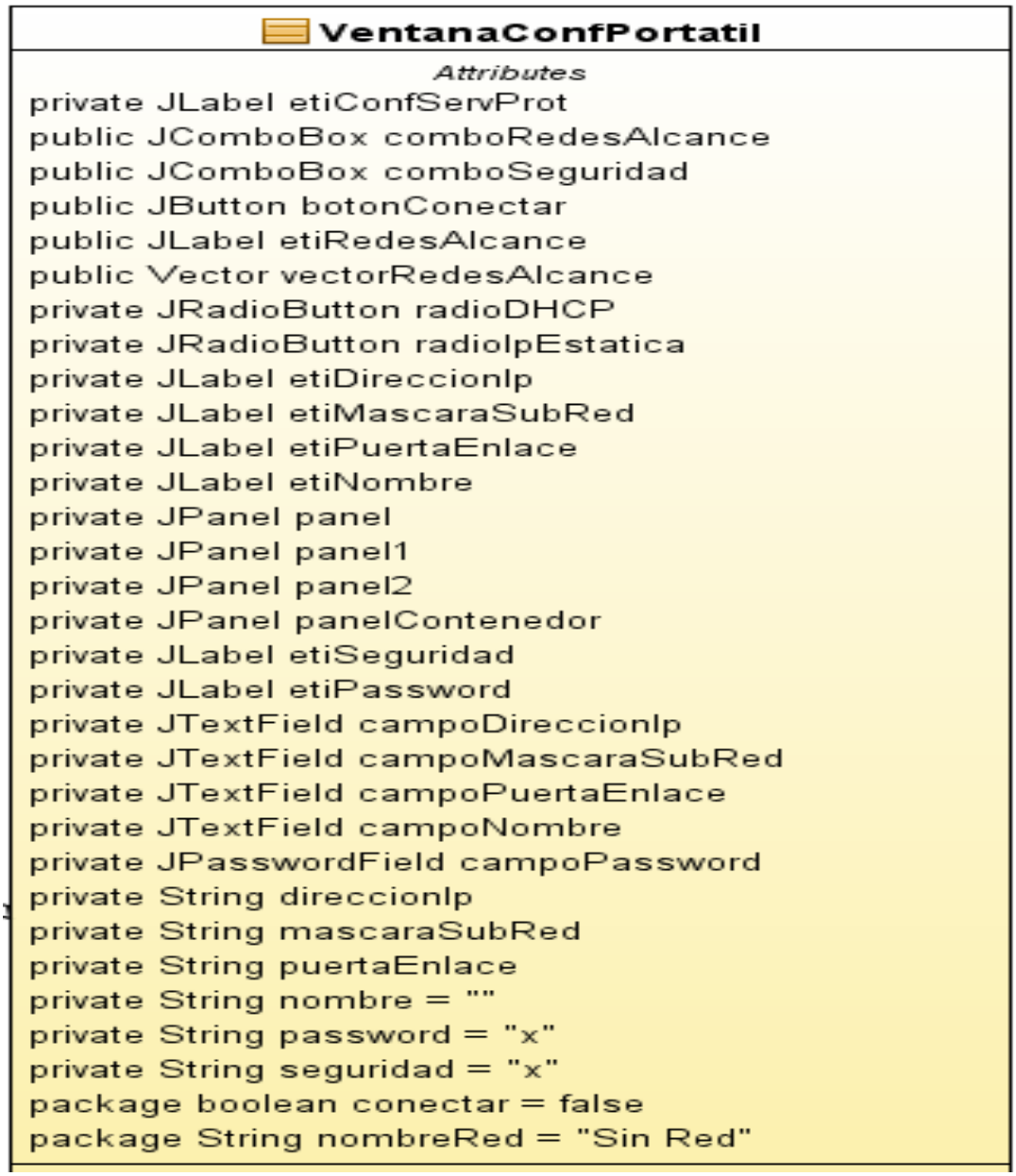
- **Diagrama de clase VentanaConfimpresora:** Esta clase permite la configuración de un dispositivo impresora, para ser implementada en el área de trabajo del simulador de seguridad de redes Wi-Fi (ver figura 17).

Figura 17. Diagrama de clase VentanaConfImpresora



- **Diagrama de clase VentanaConfPortatil:** Esta clase permite la configuración de un computador portátil, para ser implementada en el área de trabajo del simulador de seguridad de redes Wi-Fi. Se puede seleccionar el tipo de clave, nombre de red y una contraseña (ver figura 18).

Figura 18. Diagrama de clase VentanaConfPortatil



- **Diagrama de clase VentanaConfAP:** Esta clase permite la configuración de un punto de acceso, para ser implementada en el área de trabajo del simulador de seguridad de redes Wi-Fi. Se puede seleccionar el tipo de clave, nombre de red y una contraseña (ver figura 19).

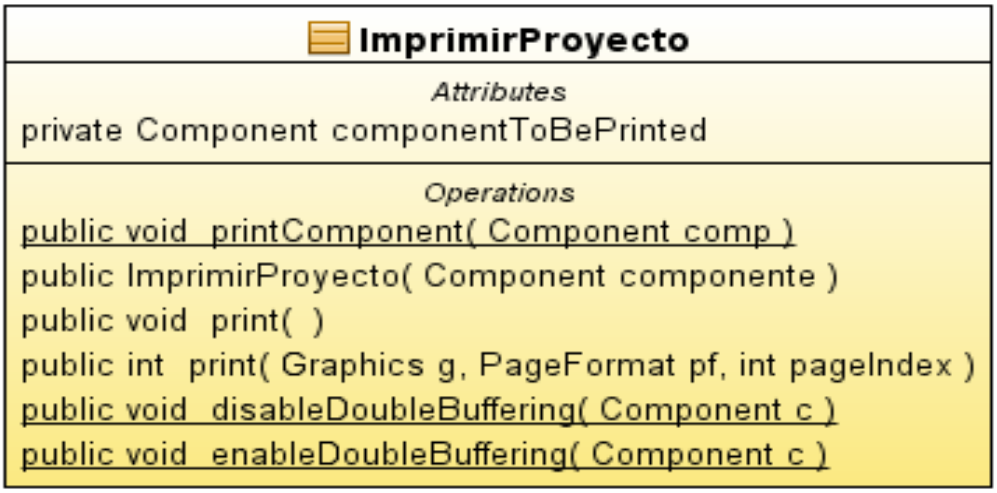
Figura 19. Diagrama de clase VentanaConfAP

- **Diagrama de clase VentanaConfEscritorio:** Esta clase permite instanciar etiquetas, campos de texto de configuración y botones, para crear objetos de los dispositivos que se deseen anexar al área de trabajo del simulador (ver figura 20).

Figura 20. Diagrama de clase VentanaConfEscritorio

- **Diagrama de clase ImprimirProyecto:** Esta clase tiene como objeto imprimir los dispositivos que se encuentren en el área de trabajo. Por medio de excepciones se establece si es posible imprimir el proyecto o por el contrario existe un error (ver figura 21).

Figura 21. Diagrama de clase ImprimirProyecto



- **Diagrama de clase Serverito:** Clase publica Serverito que crea un servidor con Sockets para crear conexiones en streams y conectar clientes (ver figura 22).

Figura 22. Diagrama de clase Serverito

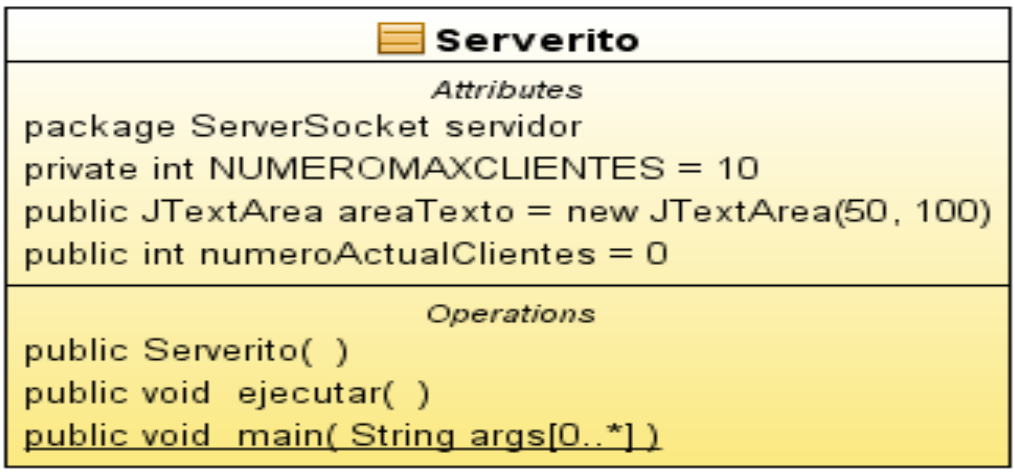
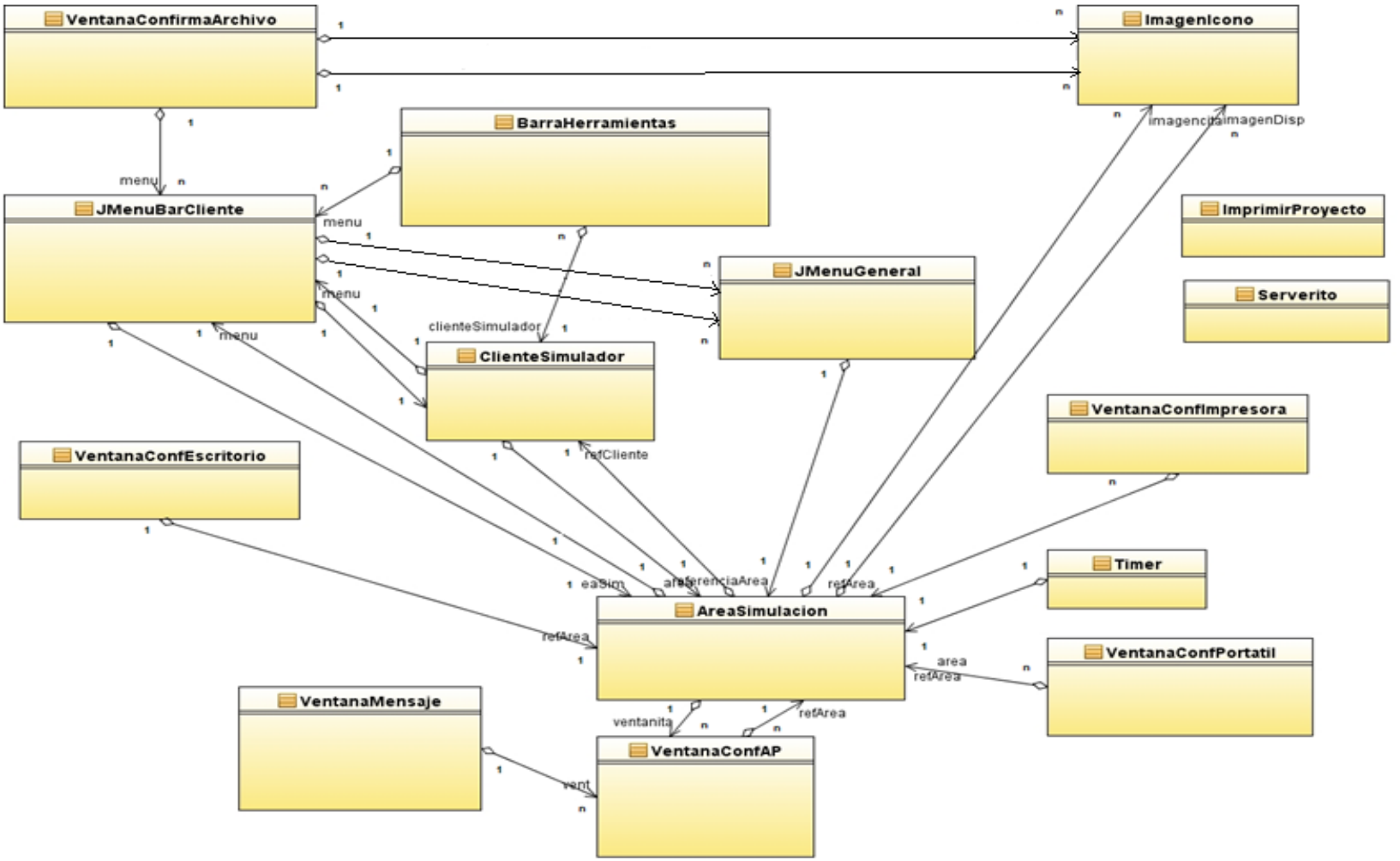


Figura 23. Diagrama de clases simulador seguridad redes Wi-Fi.



5.3.4 Diagramas de Secuencia: se realizaron diagramas de secuencia para ilustrar los objetivos del aplicativo. En las figuras 24, 25 y 26 se muestran los diagramas que permiten identificar los servicios del software y la interacción de estos en el transcurso del tiempo por medio de flechas que representan líneas de vida, las cuales van desde un punto de partida u origen, hasta un punto de destino.

5.3.5 Diagramas de Secuencia Gestión de Requisitos.

Figura 24. Diagramas de Secuencia Gestión de Requisitos para un Administrador.

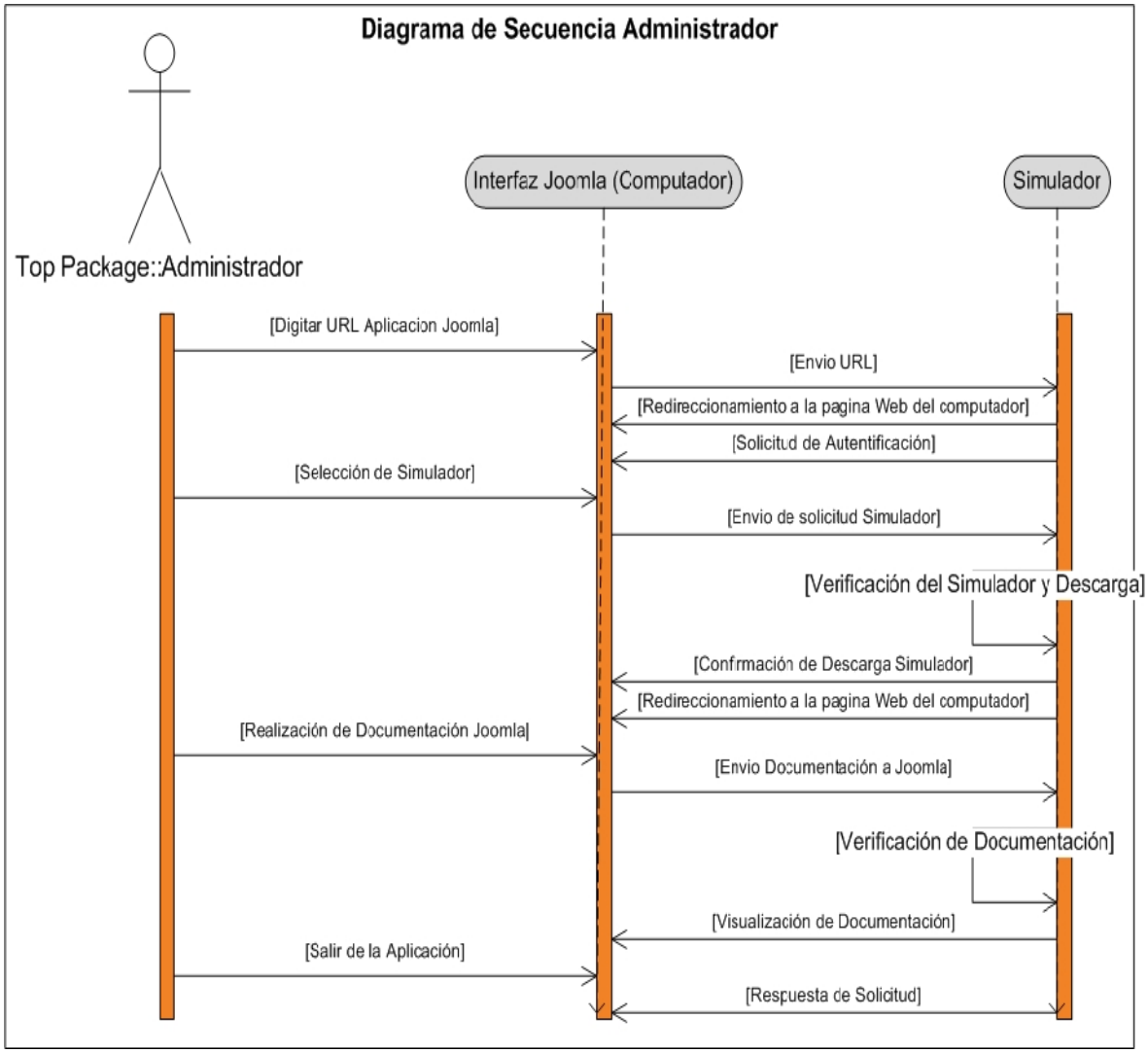


Figura 25. Diagramas de Secuencia Gestión de Requisitos para un Docente.

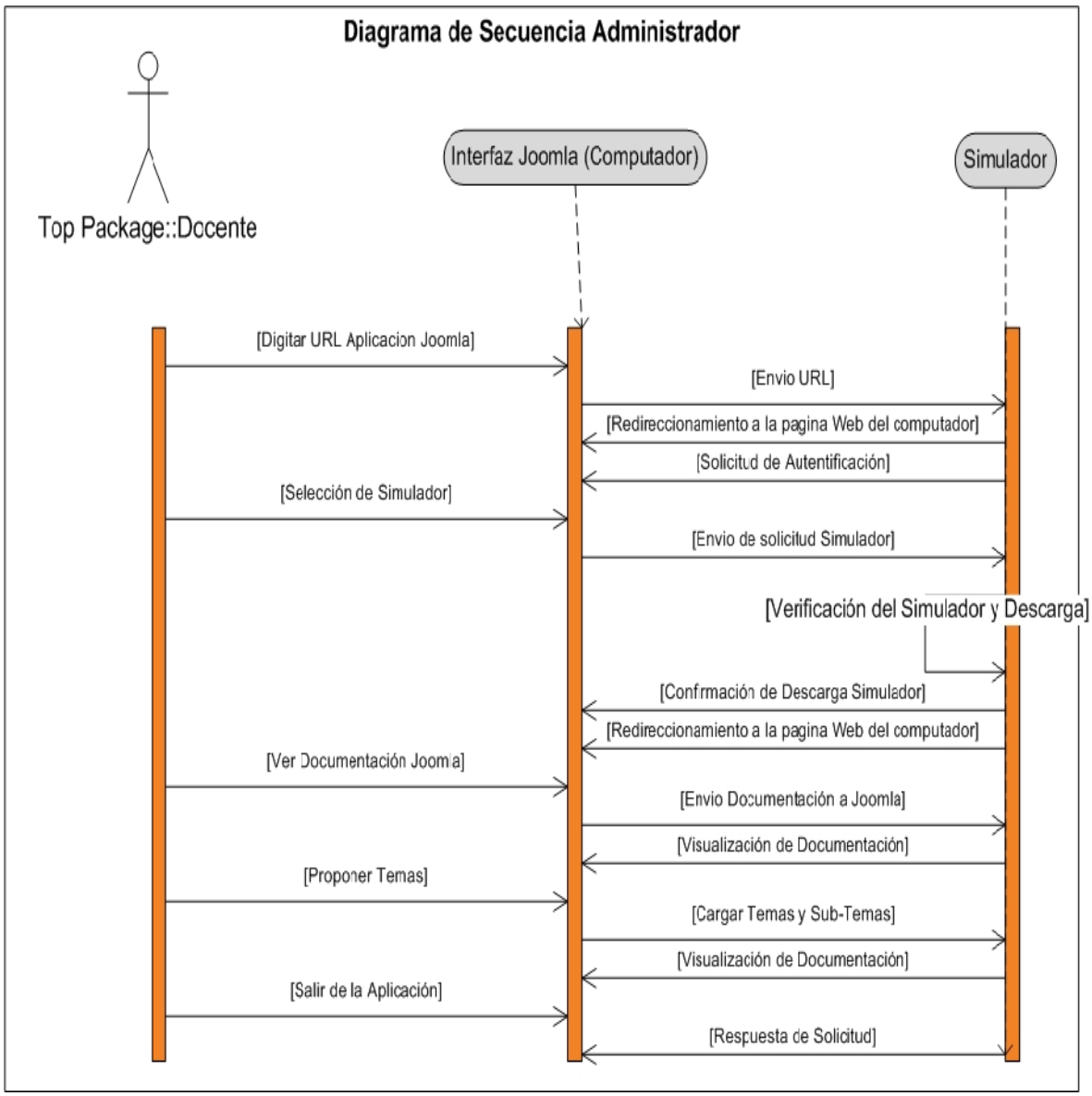
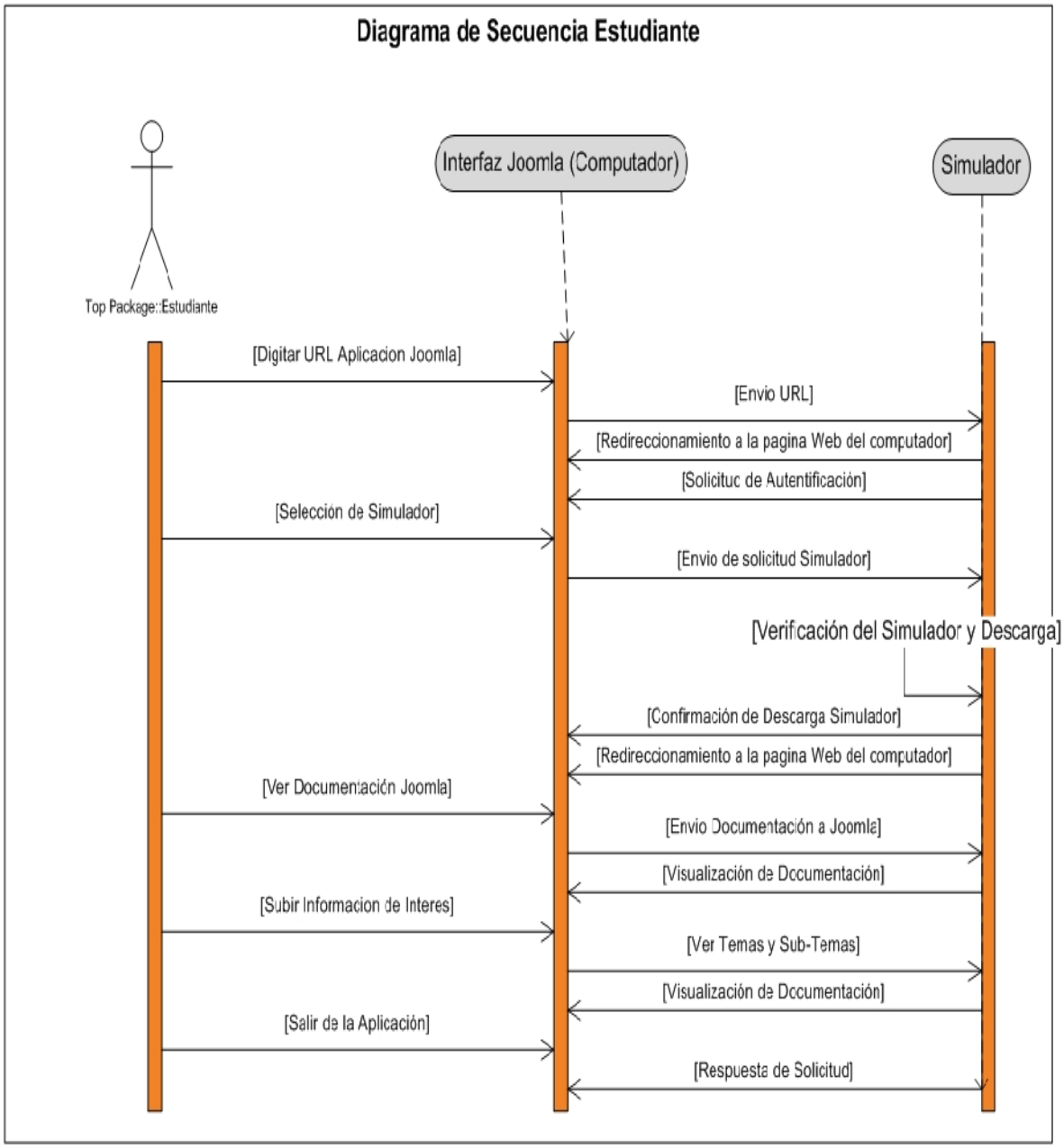


Figura 26 .Diagramas de Secuencia Gestión de Requisitos para un Estudiante



5.4 IMPLEMENTACIÓN Y PRUEBAS

La implementación del sistema se explica en archivos digitales adjuntos al proyecto y se encuentra documentación referente al código en formato html, manual de usuario y técnico, donde se explican las características del administrador de contenidos de Joomla y el simulador de seguridad de redes Wi-Fi.

Para evaluar el simulador de seguridad en redes Wi-Fi, se tiene en cuenta las dos primeras fases del modelo en cascada. Estas fases son el análisis y el diseño del aplicativo. Las pruebas que se harán son de caja negra, esto quiere decir que se evalúan aspectos funcionales, sin entrar en detalle en el código del aplicativo. A continuación se enumeran y explican los casos de pruebas funcionales que se le harán al sistema:

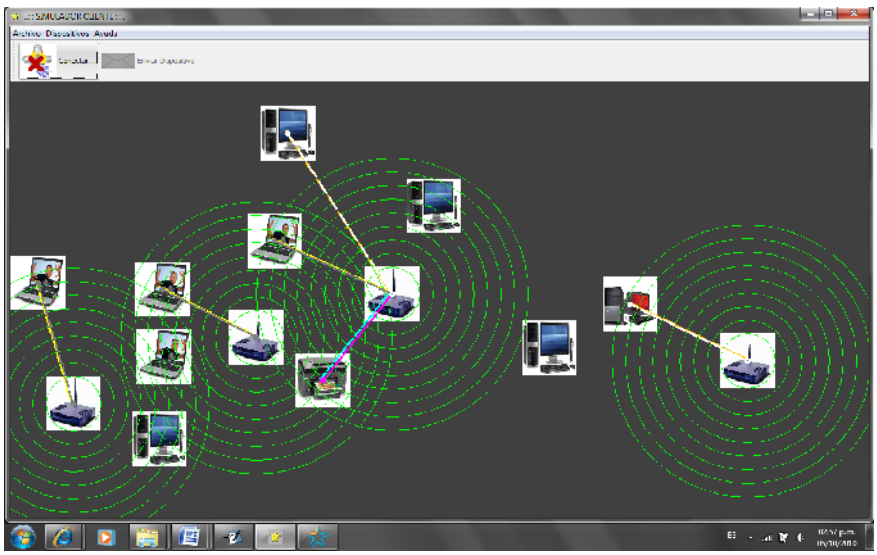
- Comprobar la adición de dispositivos de red al área de simulación.
- Configuración de Access point.
- Configuración de equipo portátil.
- Eliminar dispositivos de red.
- Guardar proyecto en disco local.
- Conexión con servidor.
- Comprobar validación de contraseñas en dispositivos de red y cliente.

5.4.1 Comprobar la adición de dispositivos de red al área de simulación:

- **Descripción**

Este caso de prueba se encarga de comprobar el funcionamiento de adición de dispositivos al área de simulación. En esta prueba se evalúa la adición de equipos portátiles, desktops, impresoras y Access Points. El entorno del cual partiremos para realizar la prueba será el área de trabajo del simulador de seguridad de redes Wi-Fi.

Figura 27. Adición de dispositivos al área de simulación.



- **Condiciones de ejecución**

Las condiciones de ejecución del caso de prueba es que el usuario compile el simulador de seguridad de redes Wi-Fi e intente acceder a la opción de nuevo dispositivo y seleccione el elemento deseado.

- **Entrada**
  - Compilar el simulador.
  - Ir a la opción Archivo/Nuevo Disp.
  - Ubicar localmente el dispositivo.
  - Seleccionar un dispositivo cliente o servidor.

- Asignar referencia del dispositivo.
- Seleccionar el dispositivo.
- Dar clic en Aceptar.
- Ir a la opción Dispositivos.
- clic en el dispositivo creado.

- **Resultado esperado**

El sistema nos presenta una interfaz que consiste en una lista de dispositivos creados con anterioridad y permite ver el dispositivo en el área de simulación.

- **Evaluación de la Prueba**

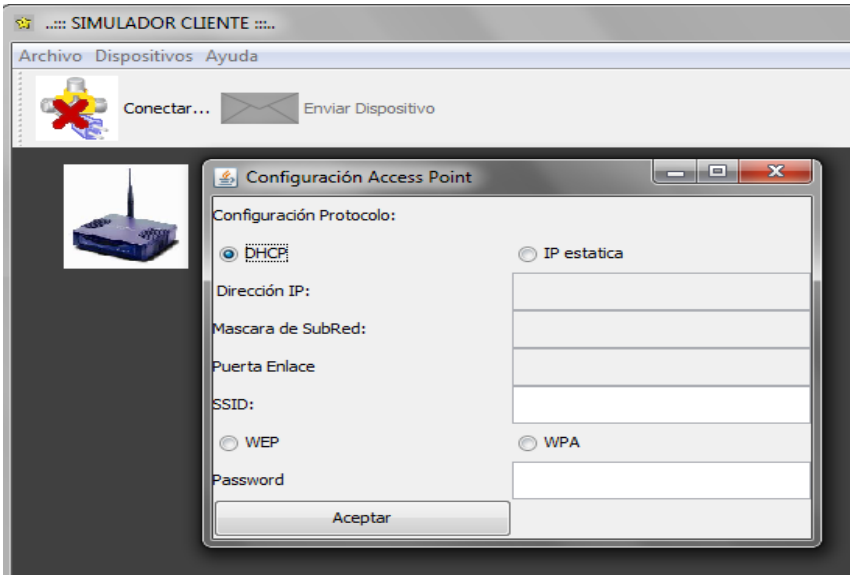
Prueba superada con éxito

5.4.2 Configuración de Access Point

- **Descripción:**

Este caso de prueba evalúa la configuración de un Access Point en el área de trabajo del simulador de seguridad de redes Wi-Fi. Asignando un nombre de red, contraseña, y un tipo de cifrado, el Access Point deberá emitir ondas.

Figura 28. Configuración de dispositivo de red



- **Condiciones de Uso.**

Ejecutar el simulador de seguridad de redes Wi-Fi, adicionar un Access Point al área de trabajo y realizar configuraciones de seguridad para establecer conexión con otros dispositivos.

- **Entrada:**
  - Adicionar un Access Point al área de trabajo.
  - Dar clic derecho sobre el dispositivo y seleccionar la opción de configurar.
  - Asignar un nombre para la red.
  - Seleccionar tipo de cifrado (WEP, WPA).
  - Asignar contraseña.
  - Dar clic en aceptar.

- **Resultado esperado:**

Configurar el Access Point para simular un área de cobertura para la red que se desee crear y que los dispositivos cercanos la reconozcan.

- **Evaluación de la prueba.**

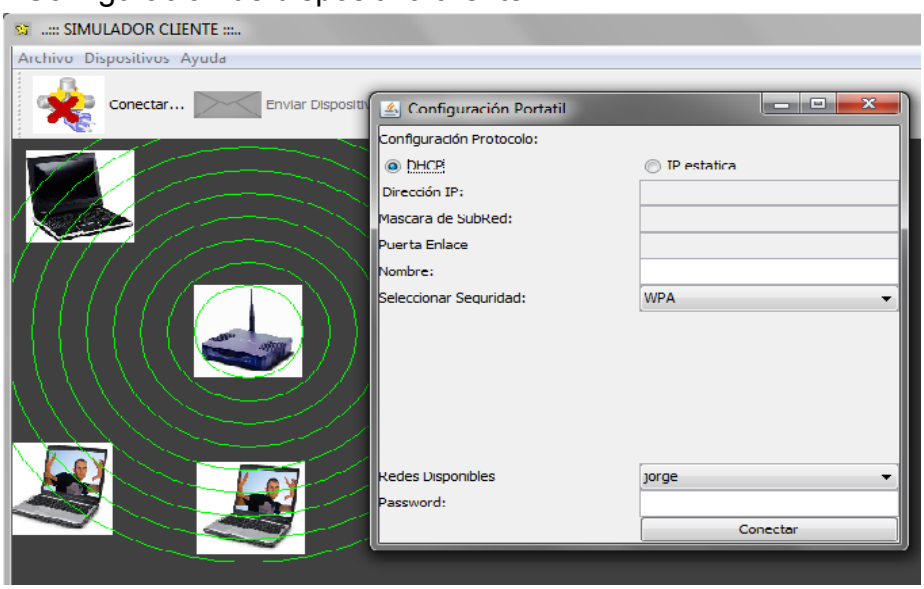
Prueba superada con éxito.

5.4.3 Configuración de un equipo portátil.

- **Descripción:**

Este caso de prueba evalúa la configuración de un equipo portátil en el área de simulación, para determinar las redes disponibles y hacer la conexión a una de ellas.

Figura 29. Configuración de dispositivo cliente



- **Condiciones de uso**

Ejecutar el simulador de seguridad de redes Wi-Fi, adicionar un portátil al área de trabajo y determinar las redes disponibles para configurar el equipo y establecer conexión con un Access Point, previamente configurado.

- **Entrada.**
  - Adicionar un equipo portátil al área de trabajo.
  - Dar clic derecho sobre el dispositivo y seleccionar la opción de configurar.
  - Asignar un nombre para el portátil.
  - Seleccionar tipo de clave (WPA, WEP).
  - Seleccionar la red a la que se desea conectar.
  - Digitar la contraseña establecida en el Access Point.
  - Dar clic en aceptar.

- **Resultado esperado:**

El equipo portátil debe establecer conexión con el Access Point seleccionado y realizar la simulación de intercambio de información entre estos dos dispositivos.

Evaluación de la prueba.

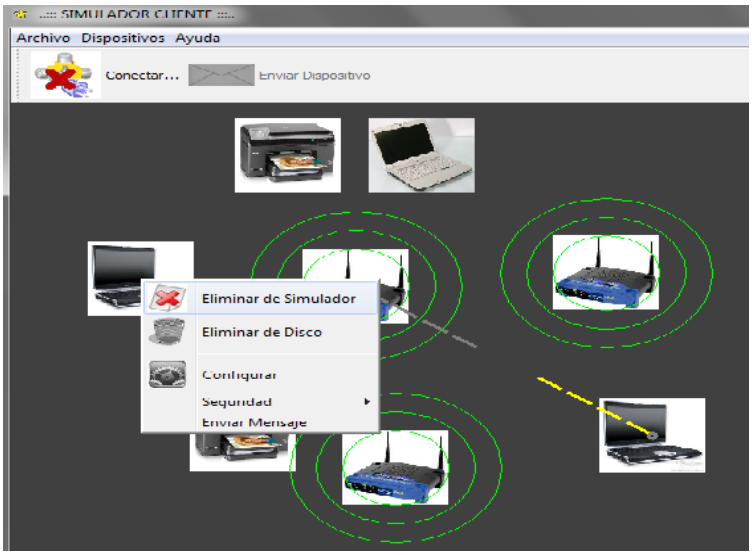
Prueba superada con éxito.

5.4.4 Eliminar dispositivos de red.

- **Descripción:**

Esta prueba permite eliminar un dispositivo de red implementado en el área de trabajo del simulador. Este tipo de dispositivo puede ser una impresora, un Access Point, un desktop o un equipo portátil.

Figura 30. Eliminar dispositivo de red del área de simulación.



- **Condiciones de uso**

Ejecutar el simulador de seguridad de redes Wi-Fi, crear la simulación de una red previamente, seleccionar el dispositivo deseado y eliminarlo del área de trabajo.

- **Entrada.**
  - Seleccionar el dispositivo.
  - Dar clic derecho.
  - Seleccionar la opción Eliminar del Simulador.

- **Resultado esperado:**

El dispositivo debe eliminarse del área de trabajo del simulador.

- **Evaluación de la prueba.**

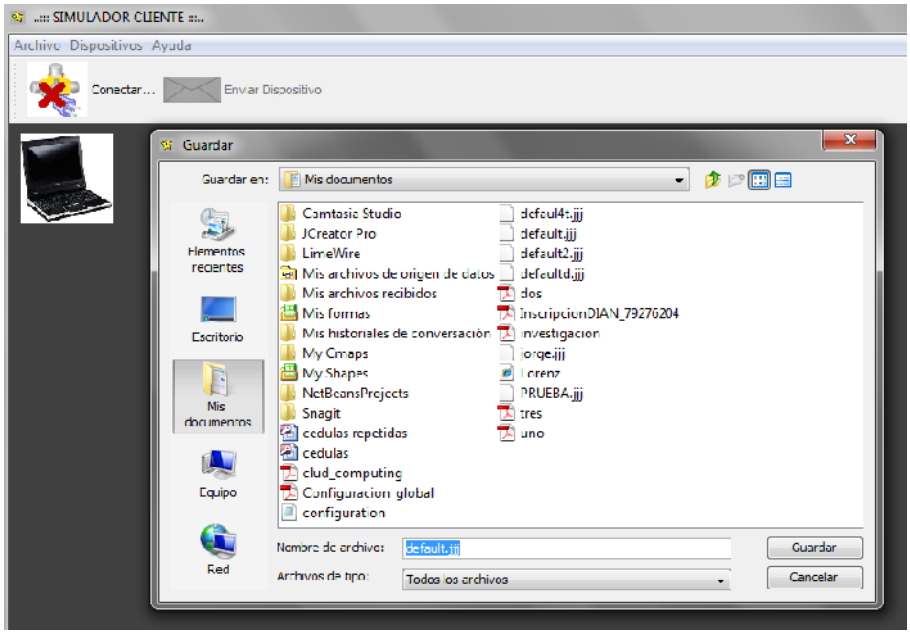
Prueba superada con éxito.

5.4.5 Guardar proyecto en disco local

- **Descripción:**

Esta prueba permite guardar un proyecto creado en el simulador. La información se guarda como archivos y se selecciona la ubicación local para su almacenamiento.

Figura 31. Guardar proyecto



- **Condiciones de Uso.**

Al ejecutar el simulador, se debe guardar el proyecto en el disco duro asignándole un nombre.

- **Entrada:**
  - Dar clic en archivo.
  - Seleccionar Guardar Proyecto.
  - Elegir la ubicación para almacenar el proyecto.
  - Asignar un nombre al archivo.
  - Dar clic en guardar.

- **Resultado esperado:**

Se espera que el proyecto se guarde en el disco duro del computador donde se ejecuta el simulador.

- **Evaluación de prueba:**

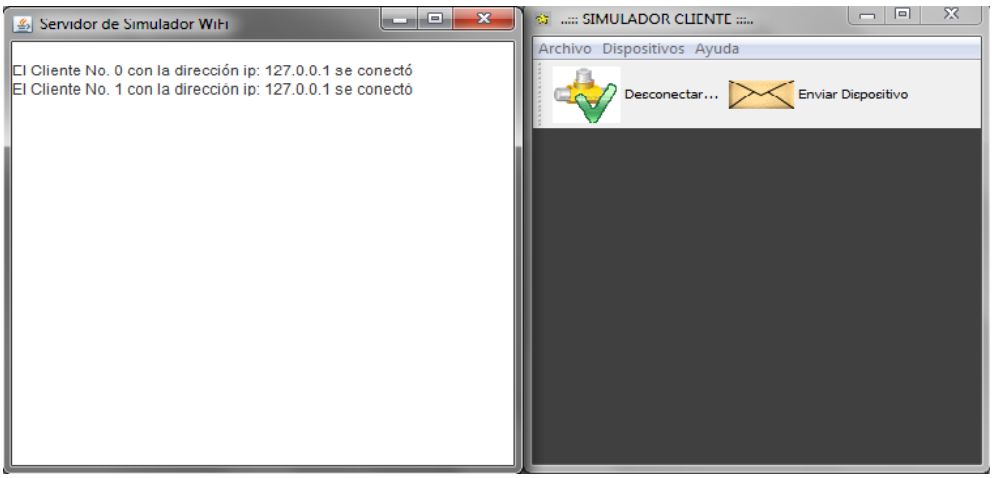
Prueba superada con éxito.

5.4.6 Conexión con servidor

- **Descripción:**

Esta prueba permite establecer una conexión con un servidor, para el intercambio de dispositivos de red; Puede realizarse local o remotamente, según el caso.

Figura 32. Conexión con un servidor local.



- **Entrada:**
  - Ejecutar el archivo serverito.
  - Ingresar al área del simulador
  - Dar clic en conectar.
  - Asignar la dirección ip 127.0.0.1

- **Resultado esperado:**

Se necesita que el cliente establezca comunicación con el servidor, luego de esto se busca que el cliente envié un dispositivo de red al servidor.

- **Evaluación de prueba:**

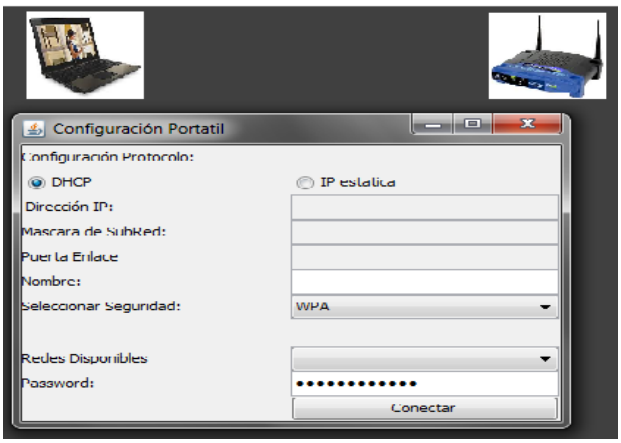
Prueba superada con éxito

5.4.7 Comprobar validación de contraseñas en dispositivos de red y cliente.

- **Descripción:**

  La siguiente validación de contraseñas, permite identificar la conectividad que puede existir entre un dispositivo de red (Access Point) y un dispositivo cliente (portátil, desktop, impresora). Por medio de esta prueba se visualiza la comunicación que se puede establecer entre los dispositivos anteriormente mencionados, por medio de líneas simuladas.

Figura 33. Validación de contraseñas.



- **Entrada:**
  - Anexar un Access Point al área de trabajo del simulador.
  - Anexar un dispositivo cliente al area de trabajo.
  - Configurar el Access Point asignando un password.
  - Digitar password en la configuración de los dispositivos cliente.
  - Dar clic en conectar.

- **Resultado esperado:**

  Si la contraseña asignada en el Access Point es igual a la digitada en los dispositivos cliente, se espera que se establezca comunicación por medio de líneas intermitentes.

- **Evaluación de prueba:**

  Prueba superada con éxito.

6. PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

En el desarrollo del proyecto se tiene en cuenta el ciclo clásico de vida de software, también llamado modelo en cascada. Este modelo se divide en fases hasta alcanzar el resultado esperado.

El enfoque que presenta este modelo, es que el inicio de cada etapa debe esperar la finalización de la fase anterior. El modelo en cascada es utilizado cuando las especificaciones de requerimientos de software son amplias.

Para el objeto virtual de aprendizaje sobre diagnóstico y seguimiento de vulnerabilidades en redes Wi-FI, el uso de este modelo permitió segmentar el proyecto en actividades donde la estrategia principal era evaluar el seguimiento del progreso del software mediante un cronograma de trabajo.

El análisis del proyecto según las fases utilizadas fueron:

- **Análisis de requerimientos**: esta fase permitió definir los requerimientos funcionales y no funcionales que tendría el aplicativo. Esta etapa es la base para la construcción del software, debido a que presenta en detalle el comportamiento del aplicativo.

  El OVA cuenta con un modulo para simular las principales características de seguridad de las redes inalámbricas Wi-Fi. Los principales requerimientos funcionales que presenta este aplicativo son:

  - Adicionar dispositivos cliente como desktops, equipos portátiles e impresoras.

  - Adicionar un dispositivo de red (Access Point).

  - Configurar los dispositivos para establecer conexión con puntos de acceso.

  - Los dispositivos cliente permiten configurar el nombre del equipo en la red, asignación de direcciones IP dinámicas (DHCP), Detección de

redes disponibles, validación de contraseñas, y el tipo de cifrado (WEP- WPA).

- Configurar los dispositivos de red utilizando DHCP, nombre de red, asignación de contraseña y tipo de cifrado (WEP, WPA).
- Eliminar dispositivos del simulador.
- Guardar un proyecto en disco local.
- Abrir un proyecto diseñado con anterioridad.
- Crear una nueva área de simulación.

El análisis permitió identificar los actores encargados de interactuar con el sistema. Dichos actores son:

- **Administradores:** Se encarga de publicar, eliminar y modificar los contenidos del OVA. Permite realizar configuraciones globales del sistema.
- **Docente:** Se encarga de publicar, eliminar y modificar los contenidos del OVA. No tiene privilegios para realizar configuraciones globales.
- **Estudiante:** Este actor visualiza los contenidos publicados en el Objeto Virtual de Aprendizaje. No puede modificar, ni eliminar contenidos. No tiene privilegios para realizar cambios globales al sistema.

- **Diseño:** el diseño permitió crear la arquitectura del sistema, para su futura implementación. En esta fase se emplearon los siguientes diagramas, para modelar el sistema:
  - **Diagrama de despliegue:** permitió identificar las tres capas que presenta el sistema. Estas capas son: presentación, lógica del negocio y capa de datos.

- **Mapa de Navegación:** se presenta la interacción con el sistema, independientemente del actor (Ver figura 9).

- **Diagrama de Clases:** Se definen las 15 clases que intervienen en el simulador de seguridad de redes Wi-Fi (ver figura 23).

- **Diagramas de Secuencia:** identifican los servicios del software y la interacción en el transcurso del tiempo, por medio de flechas que representan las líneas de vida.

- **Implementación:** la documentación del código permite determinar los atributos, métodos, variables y operaciones en general de cada clase perteneciente al simulador. Por medio de manuales de usuario y técnico se explica la estructura del OVA.

- **Pruebas:** las pruebas funcionales permitieron evaluar algunas características del simulador de seguridad de redes Wi-Fi. Se realizaron pruebas de caja negra para analizar el comportamiento de diversos módulos. Los casos de prueba fueron los siguientes:

    - Comprobar la adición de dispositivos de red al área de simulación.

    - Configuración de Access Point.

    - Configuración de equipo portátil.

    - Eliminar dispositivos de red.

    - Guardar proyecto en disco local.

    - Conexión con servidor.

    - Validación de contraseñas en dispositivos de red y cliente.

La plataforma del Objeto Virtual de Aprendizaje para el diagnóstico y seguimiento de vulnerabilidades en redes inalámbricas Wi-Fi (Joomla), permite la integración de estudiantes, docentes y administradores por medio de las siguientes herramientas:

- Foro: Los usuarios pueden registrar comentarios sobre la seguridad en redes inalámbricas Wi-Fi.

- Zona de Archivos: los estudiantes y docentes pueden descargar contenidos publicados por el administrador.

- Artículos: los docentes y administradores son los encargados de publicar artículos, documentos, videos e imágenes para orientar a los alumnos sobre las vulnerabilidades y protección de las redes inalámbricas.

- Eventos: Los usuarios registrados pueden acceder al link de eventos para conocer las actividades publicadas por docentes y administradores.

La interfaz grafica del OVA es amigable. Esto quiere decir que un usuario con pocos conocimientos en sistemas, puede familiarizarse rápidamente con la plataforma y navegar por ella.

7. CONCLUSIONES

Las nuevas tecnologías de información ofrecen herramientas y mecanismos que pueden fortalecer el proceso educativo de un alumno.

El Objeto Virtual (OVA) fomenta el aprendizaje por medio de opiniones, documentos, videos, foros y comunidad, que permiten integrar diversos puntos de vista en el tema de diagnóstico y seguimiento de vulnerabilidades en redes inalámbricas Wi-Fi.

La metodología utilizada en el desarrollo del OVA se caracteriza por tener una etapa de análisis, diseño, implementación y pruebas. Dicha metodología permitió establecer un orden o secuencia de pasos, para el desarrollo del software y la integración del Objeto Virtual de Aprendizaje para el diagnóstico y seguimiento de vulnerabilidades en redes Wi-Fi.

Por medio del aplicativo (OVA) y el desarrollo de un simulador de las principales características de seguridad en una red Wi-Fi, se da a conocer a los alumnos las causas más conocidas de riesgos a las que están expuestas las redes informáticas y sus posibles soluciones.

Conocer e identificar vulnerabilidades en las redes Wi-Fi, hace que se puedan adoptar contramedidas y establecer futuros vectores de ataque por parte de usuarios mal intencionados.

8. RECOMENDACIONES

Crear un semillero en la Universidad San Buenaventura (Bogotá) que enseñe a los alumnos las ventajas, desventajas, características y especificaciones de los Objetos Virtuales de aprendizaje.

Se debe establecer una metodología para garantizar que los contenidos publicados en los foros, temas y cursos sean enriquecedores y ayuden al rápido aprendizaje sobre el tema de interés para los usuarios finales que serian los estudiantes o profesores.

Es importante que los contenidos de cada curso, foro y tema sean bastante claros y concisos para evitar confusión por parte usuarios. Es necesaria la verificación de contenidos por parte de docentes o expertos en el área de seguridad en redes Wi-Fi, para garantizar la veracidad de la información.

Estar actualizado e informado sobre nuevas tecnologías de seguridad evaluando su impacto, la posibilidad de implementar y fortalecer a los usuarios en temas relacionados en utilizar protocolos de red inalámbrica de la forma más efectiva y segura posible para enfrentar las amenazas que aparezcan.

El aplicativo está sujeto a ser mejorado por nuevos estándares que salgan al mercado.

Se sugiere que se realicen pruebas de aprendizaje no definidas en los alcances del proyecto, para evaluar el uso pedagógico del OVA, entre docentes y alumnos.

Por último se recomienda, que el Objeto virtual de Aprendizaje para el diagnóstico y seguimiento de vulnerabilidades en redes inalámbricas Wi-fi, sea actualizado por parte de alumnos, para posibles temas de grado o proyectos integradores.

BIBLIOGRAFÍA

ACIS, EVOLUCIÓN Y MONITOREO DE LA SEGURIDAD INFORMÁTICA, Revista: Sistemas No. 110, Abril – Junio 2009.

ARIZA. Lina. Panorámica del Software Libre en Colombia. En: Sistemas. Septiembre-Noviembre, 2004, vol.90

CARRIER Brian D. IEEE SECURITY AND PRIVACY, Article: Digital Forensics work. Abril de 2009.

CARRIER Brian D. IEEE SECURITY AND PRIVACY, Article: Security Education Using Second Life. Abril de 2009.

GALLARDO Sara. "SISTEMAS: Gestión de la Inseguridad Informática, encuesta nacional. Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS). Bogotá D.C Colombia. Pág. 4-25. 2008

GALLARDO Sara. "SISTEMAS: Proyectos de Grado Ingeniería de Sistemas. Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS). Bogotá D.C Colombia. Pácanalg. 6-110. 2008

JACOBSON, Ivar; Booch, Grady; Rumbaugh James; El Proceso de Desarrollo de Software, Addison-Wesley, 1999.

MASTER MAGAZINE Noviembre de 2007[En línea]. [Consulta: noviembre 2 de 2009]. [Def. Hardware] Disponible en:www.mastermagazine.info/termino/5330.php

PICOUTO, Fernando. "Hacking y Seguridad en Internet" Alfa omega. Pág. 345-453. 2007

PRESSMAN S. Roger. Ingeniería del Software un enfoque práctico. México: Mc Graw Hill, 2006. p 958

WEBGRAFÍA

AULA. Junio de 2005 [En línea]. [Consulta: noviembre 2 de 2009]. [Def. WI-FI] Disponible en: http://www.aulaclic.es/articulos/wifi.html

Avances Tecnológicos. Octubre de 2008. [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Criptografía asimétrica] Disponible en: www.economianacional.nireblog.com/

Avances Tecnológicos. Octubre de 2008. [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Criptografía simétrica] Disponible en: www.economianacional.nireblog.com/

Comunicación Global. Febrero de 2002. [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Certificado Digital] Disponible en: www.ecvoip.biz/PCIWireless.html
Conexión activa. Febrero de 2000. [En línea].[Consulta: noviembre 2 de 2009]. [Def. Access Point] Disponible en: http://conexiaperu.com/aps.htm

DEFINICIÓN Marzo de 2008 [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Firewall] Disponible en: http://www.definicion.org/firewall.

DEFINICIÓN Marzo de 2008 [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Firma Digital Disponible en: http://www.definicion.org/firewall

DICCIONARIO INFORMÁTICO. Marzo de 2008 [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Encriptación] Disponible en: http://www.alegsa.com.ar/Dic/encriptacion.php.

Diccionario informático. Marzo de 2008 [En línea]. [Consulta: noviembre 2 de 2009]. [Def. LAN] Disponible en: http://www.alegsa.com.ar/Dic/encriptacion.php.

DICCIONARIO INFORMÁTICO. Marzo de 2008 [En línea]. [Consulta: noviembre 2 de 2009]. [Def. SSID] Disponible en: http://www.alegsa.com.ar/Dic/encriptacion.php.

Diccionario informático. Marzo de 2008 [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Troyano] Disponible en: http://www.alegsa.com.ar/Dic/encriptacion.php.

Diccionario informático. Marzo de 2008 [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Virtualización] Disponible en: http://www.alegsa.com.ar/Dic/encriptacion.php.

IEEE. Enero de 2009 [En línea]. [Consulta: noviembre 2 de 2009]. [Def. IEEE] Disponible www.ieee.org/colombia...

SITIOS ARGENTINA. Noviembre de 2009. [En línea]. [Consulta: Octubre 30 de 2009]. [Def. Pishing] Disponible en: www.sitiosargentina.com.ar/notas/Febrero.../101.htm

UNESCO Enero de 2009. [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Criptografía simétrica] Disponible en: www.unesco.org/general/spa/

UNESCO Enero de 2009. [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Unesco] Disponible en: www.unesco.org/general/spa/

ZIFLO. Abril de 2007. [En línea]. [Consulta: noviembre 2 de 2009]. [Def. Defcon] Disponible en: www.foro.ziflo.com/?topic=349

GLOSARIO

802.11b (Wi-Fi): es una extensión de alto rendimiento del estándar 802.11 para WLAN tiene una máxima transacción de 11Mbit/s y funciona con una banda de 2.4 GHz.

802.11G (WI-FI): este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22.0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias.

802.11N (WI-FI): el estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 Ghz y 5,4 Ghz. Las redes que trabajan bajo los estándares 802.11b y 802.11g, tras la reciente ratificación del estándar, se empiezan a fabricar de forma masiva y es objeto de promociones de los operadores ADSL, de forma que la masificación de la citada tecnología parece estar en camino. Todas las versiones de 802.11xx, aportan la ventaja de ser compatibles entre sí, de forma que el usuario no necesitará nada más que su adaptador Wi-Fi integrado, para poder conectarse a la red.

.

802.1X (EAP SOBRE LAN (EAPOL) PARA LAN / WLAN DE AUTENTICACIÓN Y GESTIÓN DE CLAVES): el protocolo 802.1x es clave en el llamado EAP sobre LAN (EAPOL). It is currently defined for Ethernet-like LANs including 802.11 wireless, as well as token ring LANs (including FDDI). En la actualidad está definido para Ethernet como LAN inalámbrica 802.11 incluidos, así como las redes LAN token ring (incluyendo FDDI).

ACCESS POINT: un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.

BACKUP: una copia de seguridad o backup en informática es un archivo digital, un conjunto de archivos o la totalidad de los datos considerados lo suficientemente importantes para ser conservados.

BUGS: un defecto de software (computer bug en inglés), es el resultado de un fallo o deficiencia durante el proceso de creación de programas de ordenador o computadora (software). Dicho fallo puede presentarse en cualquiera de las

etapas del ciclo de vida del software aunque los más evidentes se dan en la etapa de desarrollo y programación.

BUGTRAQ: es una lista de correo electrónico para publicación de vulnerabilidades de software y hardware. Su listado de vulnerabilidades puede servir tanto a un administrador de sistemas para enterarse de los fallos y si es posible arreglarlos, como a un cracker para atacar sistemas vulnerables".

CERTIFICADO DIGITAL: permite verificar la identidad de un ciudadano, garantizando que únicamente él puede acceder a su información personal, evitando suplantaciones. También es el elemento usado para firmar electrónicamente solicitudes o documentos.

CRACKERS: los crackers son individuos con interés en atacar un sistema informático para obtener beneficios de formas ilegales o simplemente, para provocar algún daño a la organización propietaria.

CRIPTOGRAFÍA ASIMÉTRICA: es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

CRIPTOGRAFÍA SIMÉTRICA: la criptografía simétrica es el método criptográfico que emplea una misma clave para cifrar y descifrar mensajes. Las dos partes que utilizan el sistema, puede ser de variado tipo, tienen la misma clave para utilizar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma. La seguridad reside en la clave y no en el algoritmo de cifrado, este puede ser de uso genérico.

CVE: vulnerabilidades y Exposiciones Comunes (CVE ®) es un diccionario de nombres comunes (es decir, los identificadores de CVE) para vulnerabilidades de seguridad conocidas públicamente la información, mientras que su enumeración común de configuración (CCE ™) proporciona identificadores de problemas de configuración de seguridad y las exposiciones.

DEFCON: es una de las más viejas convenciones de hackers. Se lleva a cabo generalmente en la última semana del mes de julio o la primera semana de agosto en Las Vegas.

DHCP: (sigla en inglés de Dynamic Host Configuration Protocol - Protocolo Configuración Dinámica de Servidor) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres.

ENCRIPTACIÓN: (cifrado, codificación). La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptado sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

EXPLOIT: es una pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado.

FIREWALL: (muro de fuego - cortafuego). Herramienta de seguridad que controla el tráfico de entrada/salida de una red.

FIRMA DIGITAL: una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. La firma digital no implica que el mensaje esté encriptado, es decir, que este no pueda ser leído por otras personas; al igual que cuando se firma un documento holográficamente este sí puede ser visualizado por otras personas.

HACKERS: los términos hacker y hack tienen connotaciones positivas e, irónicamente, también negativas. Los programadores informáticos suelen usar las hacking y hacker para expresar admiración por el trabajo de un desarrollador de software calificado.

HARDWARE: en computación, término inglés que hace referencia a cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con la computadora. No sólo incluye elementos internos como el disco duro, CD-ROM, disquetera, sino que también hace referencia al cableado, circuitos, gabinete, etc. E incluso hace referencia a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos.

IEEE: (institute of Electrical and Electronics Engineers). Asociación de profesionales norteamericanos que aporta criterios de estandarización de dispositivos eléctricos y electrónicos.

IETF: internet Engineering Task Force (IETF) (en español Grupo de Trabajo en Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.

LAN: (local Área Network - Red de Área Local). Interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar, limitada generalmente a un edificio. Con esta se pueden intercambiar datos y compartir recursos entre las computadoras que conforman la red.

MAC: (media Access Control o control de acceso al medio) es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una Ethernet de red.

METADATA: es data que describe otra data. Es información que describe el contenido de un archivo u objeto. Por ejemplo, una imagen digitalizada de una orden de compra es la data. La descripción de este documento es el número de la orden de compra, dirección física, nombre a quien va dirigido y fecha. Esto sería la Metadata.

METADATOS: el término metadatos describe varios atributos de los objetos de información y les otorga significado, contexto y organización.

PHREAKERS: los phreakers son intrusos especializados en sabotear las redes telefónicas para poder realizar llamadas gratuitas. Los phreakers desarrollaron las famosas cajas azules.

PISHING: es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea[1] o incluso utilizando también llamadas telefónicas.

RETINA: es una potente solución unificada y la vulnerabilidad de cumplimiento diseñado para ayudar a las organizaciones de todos los tamaños con la evaluación de vulnerabilidad, mitigación y protección. La solución se fundamenta de más de una década de innovación tecnológica de renombre mundial de eEye equipo de investigación de seguridad y es una integrada de la vulnerabilidad de extremo a extremo y la solución de cumplimiento diseñado para ayudar a las organizaciones con la protección y Conformidad, definiendo y controlando pertinentes controles de TI.

RFC: en una red informática de ingeniería, una solicitud de comentarios (RFC) es un memorando publicado por la Internet que describe los métodos, los comportamientos, la investigación, o innovaciones aplicables al trabajo de la Internet y los sistemas conectados a Internet.

SNIFFERS: los sniffers son individuos que se dedican a rastrear y tratar de recomponer descifrar los mensajes que circulan por redes de ordenadores como Internet.

SPAMMERS: los spammers son los responsables del envió masivo de miles de mensajes de correo electrónico no solicitados a través de redes como Internet, provocando el colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios.

SSID: (service Set IDentifier) es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

SSS: shadow Security Scanner es un completísimo y efectivo escáner de vulnerabilidades para la plataforma de Windows nativa, aunque también examina servidores de cualquier otra plataforma revelando brechas en Unix, Linux, FreeBSD, OpenBSD y Net BSD. Por su arquitectura, Shadow Security Scanner también descubre fallos en CISCO, HP y otros equipos de la red. Actualmente, los servicios analizados son: Definición de 'FTP'.

TROYANO: en informática, se denomina troyano o caballo de Troya (traducción literal del inglés *Trojan horse*) a un programa malicioso que bajo una apariencia inofensiva se ejecuta de manera oculta en el sistema y permite el acceso remoto de un usuario no autorizado al sistema. El término viene de la historia del Caballo de Troya en la mitología griega. Un troyano no es un virus informático, las principales diferencias son que los troyanos no propagan la infección a otros

sistemas por sí mismos y necesitan recibir instrucciones de un hacker para realizar su propósito.

VIRTUALIZACIÓN: refiere a la abstracción de los recursos de una computadora, llamada Hypervisor o VMM (Virtual Machine Monitor) que crea una capa de la abstracción entre el hardware de la maquina física (host) y el sistema operativo.

WECA: (wireless Ethernet Compatibility Alliance), es una empresa creada en 1999 con el fin de fomentar la compatibilidad entre tecnologías Ethernet inalámbricas bajo la norma 802.11 del IEEE. WECA cambió de nombre en 2003, pasando a denominarse Wi-Fi Alliance.

WEP: encriptación de privacidad (Wired Encryption Privacy), es la capacidad del estándar IEEE 802.11 para crear un nivel de seguridad análogo para las redes cableadas. Un secreto compartido que maneja la WEP es (Clave o Contraseña) para la autenticación de la red WLAN.

WI-FI: (wireless Fidelity): Conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11 (especialmente la 802.11b), creado para redes locales inalámbricas, pero que también se utiliza para acceso a Internet.

WIRELESS: la comunicación inalámbrica (inglés wireless, sin cables) es el tipo de comunicación en la que no se utiliza un medio de propagación físico alguno esto quiere decir que se utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión".

WLAN: una red inalámbrica de área local (WLAN) es un sistema de comunicación que trasmite y recibe datos utilizado ondas electromagnéticas y que proporciona conectividad inalámbrica, dentro de los edificios de la Universidad de San Buenaventura y áreas como el campus universitario.

WPA: acceso protegido Wi-Fi (WPA) lo que es, básicamente una versión previa del estándar IEEE 802.11i con la norma WPA tiene como objetivo solucionar todas las deficiencias de la WEP.

ANEXO A.

FICHA DE DATOS DEL OBJETO VIRTUAL DE APRENDIZAJE.

General	OBJETO INFORMATIVO
Título:	Objeto virtual de aprendizaje (OVA) para el diagnóstico y seguimiento de vulnerabilidades en una red inalámbrica Wi-fi.
Descripción:	TRABAJO ANTEPROYECTO DE GRADO PARA OPTAR POR EL TITULO DE INGENIERÍA DE SISTEMAS. UNIVERSIDAD DE SAN BUENAVENTURA (BOGOTÁ).
Idioma(s):	Español
Palabras Clave:	REDES WI-FI, VULNERABILIDADES, RIESGOS, SEGURIDAD, OBJETO VIRTUAL DE APRENDIZAJE.
Ciclo de Vida	
Autor(es)	CASTIBLANCO RIAÑO JORGE ALBERTO SÁNCHEZ CARRILLO JHONATHAN
Entidad(es):	Universidad de San Buenaventura (Bogotá).
Versión:	1.0
Fecha:	Octubre 1, 2010.
Técnico	
Formato:	Documento (.doc.)
Ubicación:	
Instrucciones de instalación:	Ninguna
Requerimientos:	Internet Explorer 6.0 o superior, Word 2003 o superior
Derechos	
Costo:	Libre

Derechos de Autor y otras Restricciones:	Este Objeto Virtual de Aprendizaje es desarrollado para la Universidad de San Buenaventura (Bogotá), el cual corresponde de manera respectiva, a investigadores, profesores, estudiantes y/o articulistas en los diversos medios de publicación contemplados y/o referenciados. La información asociada, únicamente podrá ser utilizada para fines académicos; por lo tanto, el usuario se compromete a usarla de forma diligente, correcta y lícita, quedando prohibida su utilización, para fines comerciales o de lucro.
Anotación	
Uso Educativo	Diseñado para divulgar vulnerabilidades en las redes WI-FI. Sirve para analizar y conocer posibles ataques en redes Wi-fi.
Clasificación	
Fuente de Clasificación:	Áreas de Conocimiento.
Ruta Taxonómica:	Ingeniería >Ingeniería de Sistemas y telecomunicaciones.

ANEXO B

MARCO REGULATORIO DE SEGURIDAD EN REDES Y ACCESO A INTERNET EN COLOMBIA

ACCIONES JURÍDICAS

-Ley 527 del 18 de Agosto de 1999

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

• **Decreto 1147 del 11 de Septiembre de 2000**

Este Decreto considera que el documento electrónico tiene la misma validez legal que los documentos en papel.

Desde la perspectiva del Derecho Informático existen diversos aspectos legales de importancia que deben ser analizados como por ejemplo:

• Seguridad y privacidad de las transmisiones

• Firma digital sustituyendo la tradicional firma escrita.

• Desmaterialización de los documentos escritos en papel.

• La naturaleza jurídica de los documentos transmitidos a distancia electrónicamente

.• Destinatario (domicilio virtual) o dirección electrónica de la Web de la persona, constituye la residencia permanente en la Web

• La responsabilidad derivada de la comisión de ilícitos penales o delitos informáticos.

• **Decreto 1524 del 24 de Julio de 2002.**

El cual tiene como objetivo regular aspectos relacionados con la comercialización de bienes y servicios a través de redes globales de información.

Dentro de los temas que regula el Decreto 1524 se encuentra el Spamming el cual es definido en dicho Decreto como el uso de los servicios de correo electrónico para difundir mensajes no solicitados de manera indiscriminada a una gran cantidad de destinatarios.

El Decreto 1524 impuso a los proveedores de servicio de Internet, proveedores de servicio de alojamiento o usuarios corporativos, la obligación de implementar sistemas internos de seguridad para su red.

Con el fin de evitar el acceso no autorizado a sus redes, la realización del spamming o que desde sistemas públicos personas inescrupulosas tengan acceso a su red, con el fin de difundir en ella contenido relacionado con Pornografía Infantil.

Es decir que El Decreto 1524 no se pronunció sobre los aspectos que realmente implican el mail spamming sino que lo reguló tangencialmente bajo la única óptica de la Pornografía Infantil, dejando un vacío en la materia que olvida el legítimo interés de los sectores de Comunicaciones, Industrial, Comercial y Financiero, los cuales requieren realizar la comercialización de sus productos y servicios por medio del correo electrónico.

• Sanciones que están determinadas

En Colombia el acceso abusivo a un sistema informático se castiga con multa.

La violación ilícita de comunicación o correspondencia oficial con 3 a 6 años de cárcel.

La utilización ilícita de equipos transmisores o receptores (Wi-Fi) se penaliza con 1 a 3 años.

La violación ilícita de comunicaciones con 2 a 4 años.

El delito de sabotaje con uno a seis años y multa de 5 a 20 salarios mínimos legales mensuales vigentes.

• Multas estipuladas en esta Ley

–La Superintendencia de Industria y Comercio podrá aplicar una multa de hasta por el equivalente a dos mil (2.000) salarios mínimos legales mensuales vigentes (320.000 US) dependiendo de la gravedad de la infracción, a toda persona natural o jurídica que envíe mensajes de correo electrónico en contravención de la presente ley.

La venta de base de datos y de direcciones electrónicas obtenidas ilegalmente y recolección fraudulenta o maliciosa de direcciones de correo electrónico de sitios de acceso público tales como sitios de charla ("Chat rooms"), directorios públicos, grupos receptores de noticias ("newsgroups") y servicios de perfiles en línea, sin la autorización del titular del correo electrónico o del operador del sitio de acceso público, será sancionada con una multa hasta por el equivalente a mil (1.000) salarios mínimos legales mensuales vigentes (160.000 US).

La creación, venta, préstamo, intercambio o cualquier tipo de transferencia de listas de direcciones electrónicas para el envío de mensajes comerciales no solicitados cuando dicha lista haya sido creada ilegalmente o sin el consentimiento del receptor o destinatario del correo electrónico también será sancionada con una multa hasta por el equivalente a mil (1.000) salarios mínimos legales mensuales vigentes (160.000 US), sin perjuicio del decomiso de los productos y/o la clausura del local a que hubiere lugar:[14] …

Con lo anterior se evidencia que la seguridad en los sistemas de información cada día se hacen más seguros, a través de leyes y reglamentación, sin embargo y en comparación con otros países, las penas en Colombia por delitos informáticos son flexibles y falta aún mucho por aplicar.

[14] Ministerio de Comunicaciones. Enero de 2009. [En línea].[Consulta: Septiembre 24 de 2009. Disponible en:<http://www.aseta.org/seminarios/ciberseguridad/LGallego-seguridad%20en%20Redes%20e%20Internet%20Colombia.pdf>

Derechos de autor y protección legal del software

Los derechos de autor y protección legal del software se utilizan para defender las creaciones de cada individuo y dar la patente para que estos puedan defenderla y venderla si desean.

La legislación que rige los derechos de autor para el software en Colombia, se define en:

Ley 23 de 1982
Ley 44 de 1993
Ley 35 de 1993 del G-3, articulo 18, párrafo 13

Decreto 1360 régimen común sobre derechos de autor y derechos conexos- Articulo 1 al 8, donde se manifiesta que las obras de soporte logico(software) se consideran como una creación propia de dominio literario y los pasos a seguir para la inscripción ante el Registro Nacional del derecho de Autor.
Decreto 351 régimen común sobre derechos de autor y derechos conexos- Capítulos I al XV, donde manifiesta los decretos que tenemos como titulares de la obra, derechos morales y derechos patrimoniales.

RESOLUCIÓN NÚMERO 1689 DE 12 DE JUNIO DE 2007 PERMITIR LA LIBRE UTILIZACIÓN DE DISPOSITIVOS CON ANTENAS OMNIDIRECCIONALES Y POTENCIAS SUPERIORES A 100 MW

LA MINISTRA DE COMUNICACIONES[15]

En ejercicio de sus facultades legales y en especial las que le confiere la Ley 72 de 1989, El Decreto-Ley 1900 de 1990, el Decreto 1620 de 2003, y CONSIDERANDO: Que el artículo 75 de la Constitución Política establece que el espectro electromagnético es un bien público inenajenable e imprescriptible sujeto a la gestión y control del Estado y que se garantiza la igualdad de oportunidades en el acceso a su uso;

Que los artículos 101 y 102 de la Constitución Política establecen que el espectro radioeléctrico es un bien público que forma parte de Colombia y pertenece a la Nación;

Que el artículo 18 del Decreto 1900 de 1990 establece que el espectro electromagnético es de propiedad exclusiva del Estado, cuya gestión, administración y control corresponden al Ministerio de Comunicaciones;

Que el artículo 19 del Decreto 1900 de 1990 señala que las facultades de gestión, administración y control del espectro electromagnético comprenden, entre otras, las actividades de planeación y coordinación, la fijación del cuadro de frecuencias, la asignación y verificación de frecuencias, el otorgamiento de permisos para su utilización, la protección y defensa del espectro radioeléctrico, la comprobación técnica de emisiones radioeléctricas, el establecimiento de condiciones técnicas de equipos terminales y redes que utilicen en cualquier forma el espectro

[15] Ministerio de Comunicaciones. Junio de 2007. [En línea].[Consulta: Enero 4 de 2010. Disponible en: http://www.mintic.gov.co/mincom/documents/portal/documents/root/Res1689de2007.pdf>

radioeléctrico, la detección de irregularidades y perturbaciones, y la adopción de medidas tendientes a establecer el correcto y racional uso del espectro radioeléctrico, y a restablecerlo en caso de perturbación o irregularidades;

Que la Resolución 689 de 2004 atribuyó unas bandas de frecuencias para su libre utilización dentro del territorio nacional, mediante sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia.
Que la Resolución 689 de 2004 en su artículo 9º postuló:
"Artículo 9.- ANTENAS OMNIDIRECCIONALES. La utilización de antenas omnidireccionales solo será permitida en sistemas inalámbricos cuya potencia radiada sea menor o igual a 100 mW. Los sistemas que excedan esta potencia deberán emplear antenas direccionales con un ancho de lóbulo no mayor a 90 grados".

Página 2 de la Resolución: "Por la cual se modifica la Resolución 689 del 21 de abril de 2004".

RESOLUCIÓN NÚMERO 1689 DE 12 JUN 2007

Que en la actualidad existen internacionalmente múltiples y diversos aparatos y dispositivos inalámbricos de banda ancha y baja potencia que utilizan antenas omnidireccionales con potencias iguales o algo superiores a los 100 mW, que cumplen con las demás disposiciones de la Resolución 689 de 2004.
Que dados los avances tecnológicos en la materia, la anterior limitación restringe el uso libre del espectro para la utilización de aparatos y dispositivos inalámbricos de banda ancha y baja potencia y la comercialización de los mismos en el país, por consiguiente se hace necesario modificar la Resolución 689 mencionada. En consideración de lo anterior,

RESUELVE: Artículo 1º. DEROGATORIA.

Derogase el Artículo 9 de la Resolución 689 del 21 de abril de 2004, de acuerdo con las consideraciones de la parte motiva de la presente Resolución.

Artículo 2º. VIGENCIA. Esta resolución rige a partir de su publicación.

PUBLÍQUESE Y CÚMPLASE

Dado en Bogotá, D. C., a los 12 DE JUNIO DE 2007

LA MINISTRA DE COMUNICACIONES

Original firmado por:

MARIA DEL ROSARIO GUERRA DE MESA

BANDA DE 900 MHZ UTILIZADA PARA EL ACCESO FIJO INALÁMBRICO EN TODO EL PAÍS. DE ESTA FORMA, SE CONTARÁ CON MAYOR ESPECTRO CONTINUO PARA EL SERVICIO DE TPBCL Y TPBCLE[16]

En el ejercicio de sus facultades legales y en especial de las que le confiere la Ley 72 de 1989, el Decreto-Ley 1900 de 1990, el Decreto 1620 de 2003, y CONSIDERANDO:

Que el artículo 75 de la Constitución Política establece que el espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado y que se garantiza la igualdad de oportunidades en el acceso a su uso.

Que los artículos 101 y 102 de la Constitución Política establecen que el espectro radioeléctrico es un bien público que forma parte de Colombia y pertenece a la Nación.

[16] Ministerio de Comunicaciones. Junio de 2007. [En línea].[Consulta: Enero 5 de 2010. Disponible en: http://www.mintic.gov.co/mincom/documents/portal/documents/root/Res1715de2007.pdf>

Que el artículo 1º de la Ley 72 de 1989 establece que el Gobierno Nacional, por intermedio del Ministerio de Comunicaciones, adoptará la política general del sector de comunicaciones y ejercerá las funciones de planeación, regulación y control de todos los servicios del sector.

Que el artículo 4º de la Ley 72 de 1989 establece que los canales radioeléctricos y demás medios de transmisión que Colombia utiliza o pueda utilizar en el ramo de las telecomunicaciones son propiedad exclusiva del Estado.

Que el artículo 18 del Decreto-Ley 1900 de 1990 expresa que el espectro electromagnético es de propiedad exclusiva del Estado y, como tal, constituye un bien de dominio público, inajenable e imprescriptible, cuya gestión, administración y control corresponden al Ministerio de Comunicaciones. Que según lo dispuesto en el artículo 19 del Decreto-Ley 1900 de 1990, las facultades de gestión, administración y control del espectro electromagnético comprenden, entre otras, las actividades de planeación y coordinación, la fijación del cuadro de frecuencias, la asignación y verificación de frecuencias, el otorgamiento de permisos para su utilización, la protección y defensa del espectro radioeléctrico, la comprobación técnica de emisiones radioeléctricas, el establecimiento de condiciones técnicas de equipos terminales y redes que utilicen en cualquier forma el espectro radioeléctrico, la detección de irregularidades y perturbaciones, y la adopción de medidas tendientes a establecer el correcto y racional uso del espectro radioeléctrico, y a restablecerlo en caso de perturbación o irregularidades.
Que la Resolución 0526 del 26 de abril de 2002 atribuyó las bandas de frecuencias para la operación de los sistemas de acceso fijo inalámbrico como elemento de la red telefónica pública básica conmutada (RTPBC) para la prestación del servicio de Telefonía Pública Básica Conmutada Local y/o Local

Extendida, y estableció disposiciones relativas a los procedimientos para el otorgamiento de los permisos.

Página 2 de la Resolución:
"Por la cual se atribuyen unas bandas de frecuencias del espectro radioeléctrico, para el Acceso Fijo Inalámbrico como elemento de la Red Telefónica Pública Básica
Conmutada (RTPBC), y se dictan otras disposiciones."

RESOLUCIÓN NÚMERO 1715 DE 14 DE JUNIO DE 2007
Que conforme a la Resolución 526 de 2002, los permisos para el uso del espectro radioeléctrico para acceso fijo inalámbrico, se otorgarán en virtud de actuación administrativa de oficio por el Ministerio de Comunicaciones, la cual se iniciará por decisión del Ministerio o a solicitud de parte en ejercicio del derecho de petición en interés general.

Que mediante la Resolución 1277 de 2005 "Por la cual se adoptan medidas en materia de ordenamiento técnico del espectro radioeléctrico y se dictan otras disposiciones", el Ministerio de Comunicaciones resolvió no otorgar nuevos permisos para el uso del espectro, en las siguientes bandas de frecuencias, hasta tanto realice la planeación y el reordenamiento del espectro en las mismas:

BANDA	ANCHO DE LA BANDA
Banda de 894,6750 a 894,9925 MHz	0,3175 MHz
Banda de 897,1375 a 897,5000 MHz	0,3625 MHz
Banda de 897,5000 a 901,0000 MHz	3,5000 MHz
Banda de 902,0000 a 905,0000 MHz	3,0000 MHz
Banda de 942,5000 a 950,0000 MHz	7,5000 MHz
Banda de 908,0000 a 915,0000 MHz	7,0000 MHz
Banda de 953,0000 a 960,0000 MHz	7,0000 MHz
Banda de 3425 a 3450 MHz	25,0000 MHz
Banda de 3475 a 3500 MHz	25,0000 MHz
Banda de 3525 a 3550 MHz	25,0000 MHz
Banda de 3575 a 3600 MHz	25,0000 MHz

Que la Resolución 2064 de 2005 atribuyó dentro del territorio nacional, a título primario al servicio fijo radioeléctrico, para la operación de los sistemas de Distribución Punto a Punto y Punto Multipunto para Acceso de Banda Ancha Inalámbrica, la banda de frecuencias radioeléctricas comprendida entre los 3 400 MHz a los 3 600 MHz, y ordenó reubicar en otras bandas de frecuencias a aquellos operadores que tuvieran asignadas frecuencias o bandas de frecuencias radioeléctricas en esta banda frecuencias. Que se hace necesario atribuir y planificar unas bandas de frecuencias del espectro radioeléctrico para el Acceso Fijo Inalámbrico como elemento de la Red Telefónica Pública Básica Conmutada (RTPBC), con el fin de permitir la reubicación de operadores y la continuidad de los procedimientos para el otorgamiento de los permisos para el derecho al uso del espectro radioeléctrico dedicado a los sistemas de Acceso Fijo Inalámbrico.

En consideración de lo anterior,

RESUELVE

Artículo 1º. ATRIBUCIÓN Y PLANEACIÓN. Se atribuye dentro del territorio nacional, para la operación de los sistemas de Acceso Fijo Inalámbrico, como elemento de la Red Telefónica Pública Básica Conmutada (RTPBC), las siguientes bandas de frecuencias radioeléctricas, en las condiciones establecidas por esta Resolución, y se ordena su inscripción en el Cuadro Nacional de Atribución de Bandas de Frecuencias:

BANDA	RANGO MHz	BANDA	RANGO MHz	ANCHO DE BANDA
A1	894,000 A 895,225	A1'	939,000 A 940,225	2 X 1,225 MHz
A2	895,525 a 896,000	A2'	940,525 a 941,000	2 x 0,475 MHz
A3	897,125 a 901,225	A3'	942,125 a 946,225	2 x 4,100 MHz
A4	901,525 a 902,225	A4'	946,525 a 947,225	2 x 0,700 MHz
C	908,000 a 911,500	C'	953,000 a 956,500	2 x 3,500 MHz
D	911,500 a 915,000	D'	956,500 a 960,000	2 x 3,500 MHz

Página 3 de la Resolución: “Por la cual se atribuyen unas bandas de frecuencias del espectro radioeléctrico, para el Acceso Fijo Inalámbrico como elemento de la Red Telefónica Pública Básica Conmutada (RTPBC), y se dictan otras disposiciones.”

RESOLUCIÓN NÚMERO 1715 DE 14 DE JUNIO DE 2007

Para la operación por Separación Dúplex por División de Frecuencia, las bandas o rangos de frecuencias se planifican de manera pareada con separación de 45 MHz entre frecuencias de transmisión y recepción. Las bandas de frecuencias quedan atribuidas al servicio radioeléctrico fijo, para el Acceso Fijo Inalámbrico, a título primario, y compartidas a título secundario con las aplicaciones y servicios previstos en el Cuadro Nacional de Atribución de Bandas de Frecuencias, adoptado mediante Decreto 555 de 1998.

Artículo 2º. DISTRIBUCIÓN. Las bandas de frecuencias radioeléctricas atribuidas y planificadas por la presente Resolución, se distribuyen y disponen para su operación en áreas de servicio municipal, conforme lo dispuesto por la Resolución 526 de 2002.

Artículo 3º. El Ministerio de Comunicaciones podrá iniciar actuaciones administrativas para otorgar permisos para el uso del espectro radioeléctrico con la utilización de sistemas de Acceso Fijo Inalámbrico en las bandas atribuidas y contempladas por la presente Resolución, de conformidad con lo dispuesto en la Resolución 526 de 2002.

Artículo 4º. Las bandas de 902,225 a 908,000 y de 947,225 a 953,000 quedan reservadas hasta tanto el Ministerio de Comunicaciones realice un reordenamiento del espectro en dichos rangos de frecuencias. En estas bandas de frecuencias no se otorgarán nuevos permisos para el uso del espectro radioeléctrico a título primario.

Articulo 5º. La presente Resolución rige a partir de su publicación y deroga las normas que le sean contrarias, en especial la Resolución 1277 de 2005.

PUBLÍQUESE Y CÚMPLASE Dada en Bogotá, D. C., a los 14 DE JUNIO DE 2007
LA MINISTRA DE COMUNICACIONES
Original firmado por
MARIA DEL ROSARIO GUERRA DE MESA

ANEXO C
SEGURIDAD INFORMÁTICA EN COLOMBIA TENDENCIAS 2008.

La encuesta sobre la seguridad informática en Colombia evaluó los siguientes temas:

- **Demografía**: identificar los sectores que participaron en el estudio.

- **Presupuestos**: las organizaciones cuanto destinan económicamente a la seguridad de la información.

- **Fallas de seguridad**: en esta sección se evalúan las fallas más frecuentes que se evidencian en la seguridad de la información.

- **Herramientas y prácticas de seguridad**: en esta sección de la encuesta, el objetivo general era clasificar que practicas o sistemas de seguridad se implementaban en las diversas organizaciones evaluadas.

- **Políticas de Seguridad**: en este segmento de la encuesta se buscaba indagar sobre la formalidad de las políticas de seguridad en las organizaciones.

En el artículo se muestran los resultados (en porcentajes) de la encuesta, los cuales presentan aproximadamente una confianza del 93%, entre 1800 participantes de la estadística, lo que significa un estudio importante para la valoración de resultados. Los sectores que intervinieron en dicha estadística, representan una población confiable, por tratarse de sectores que intervienen directa e indirectamente con la protección de la información. Se establece que sectores como la Banca, educación, vigilancia, servicios de seguridad informática entre otros, son los sectores con mayor participación en el 2008. Esto se debe a

que la protección de la información en dichos sectores, se hace imprescindible para el funcionamiento de las entidades o compañías que representan.

Otro aspecto que es vital para la investigación, es la evaluación realizada a las dependencias organizacionales de áreas de seguridad informática. Los resultados son los siguientes

Tabla 34 Dependencia Organizacional del área de Seguridad Informática

	2002%	2003%	2004%	2005%	2007%	2008%
Auditoría interna	5	3,9	6,1	7	4,8	5,56
Director de Seguridad Informática	11,9	14,7	10,2	18	20,5	25,25
Director Departamento de Sistemas/Tecnología	60,4	52,9	53,8	39	44,6	38,89
Gerente Ejecutivo	4	2	1,5	4	0,6	1,52

Fuente: Sistemas, ACIS, No. 105 Abril- junio 2008 P.43.

En los resultados que se obtuvieron en la encuesta se muestra un aumento significativo del cargo de director de seguridad de la información, con una disminución poco evidente en el área de tecnología. Analizando los resultados obtenidos, la seguridad de la información continua ganando terreno pero aún falta mayor compromiso en algunas aéreas de las organizaciones.

Como se evidencia en este estudio, al pasar los años, el incremento de capacitación de los empleados involucrados en la seguridad de las redes, tiene que ser cada vez más estricta, ya que en Colombia se están exigiendo más de dos años de experiencia en seguridad informática. Es por este motivo que el proyecto de un Objeto Virtual de Aprendizaje sobre el diagnóstico y seguimiento de vulnerabilidades es viable para la orientación de futuros administradores de redes inalámbricas.

Otro punto que es importante resaltar es el porcentaje de certificaciones en seguridad informática entre los años 2007 y 2008, en los que se basa el estudio anteriormente citado. Los resultados obtenidos de la encuesta a varios sectores productivos del país, evidencian el ligero incremento en las certificaciones evaluadas con respecto a la seguridad en redes informáticas. Los resultados se presentan a continuación:

Tabla 35. Porcentaje de encuestados que tienen una Certificación en seguridad informática

	2007	2008
Ninguna	60,3	36,5
CISSP	20,7	19,2
CISA	14,9	13,3
CISM	9,9	13,8
CFE	0,8	3,94
CIFI	5,8	1,97
CÍA	10,7	4,43
Security+	-	5,91
Otras: Especializaciones en Auditoría de Sistemas, Especializaciones en Seguridad Informática, Diplomados en Seguridad Informática, Auditor Líder BS7799, Certified Ethical Hacking, CCNA, CCSP, GSEC, MCSE, etc.	18.2	13.8

Fuente: Ibíd., p.44.

Según los encuestados, son pocos los que dicen tener una certificación en temas tales como, auditoria, fraude, seguridad informática o informática forense. Sin embargo analizando los datos se ve un leve incremento en certificaciones como la CISM (Certified Information Security Manager) y CFE, (Certified Fraud Examiner). La primera certificación es exclusiva para directores de seguridad de la información, y para aquellos miembros de las organizaciones que van con la dirección del negocio. La certificación CFE es basada en la detección y prevención de fraudes informáticos. En Colombia es necesaria la capacitación sobre seguridad en las redes inalámbricas, debido a la evolución que tienen día a día las organizaciones a niveles tecnológicos.

Es importante resaltar que la capacitación en el tema de la seguridad informática, es vital para el mantenimiento y desarrollo de cualquier organización, debido a las decisiones que se adoptan a partir de la información.

Siguiendo con el análisis del artículo, los resultados que se obtuvieron a la pregunta, ¿Qué tan importante son las certificaciones en seguridad informática?, se determinó que un alto porcentaje de actores participantes en la seguridad de las redes informáticas, respondieron que las certificaciones son vitales para las organizaciones, y que es de gran importancia para la protección de la información.

Por último y para concluir con la investigación, se presentará las tablas con resultados importantes de la encuesta, lo que nos da una idea clara de por qué es necesaria la capacitación en el tema de la seguridad informática en redes informáticas y el por qué de la implementación del Objeto virtual de aprendizaje sobre el diagnóstico y seguimiento de vulnerabilidades en las redes inalámbricas Wi-Fi.

Las tablas presentan los siguientes datos:

¿En qué temas se concentra la inversión en seguridad informática?

Tabla 36. Inversión en seguridad informática

	2002%	2003%	2004%	2005%	2007 %	2008%
Protección de la red	19,3	22,7	20,6	19	74,1	75,9
Proteger los datos críticos de la organización	19,8	19,5	18,8	18	62	61,1
Proteger la propiedad intelectual	8,9	3,7	6,1	6	21,1	30
Proteger el almacenamiento de datos de clientes	12,8	13,7	11,7	12	47,6	47,8
Concientización/formación del usuario final	7,8	7,4	9,2	8	28,3	33,5
Comercio/negocios electrónicos	4,7	4	6,5	5	10,8	21,2
Desarrollo y afinamiento de seguridad de las aplicaciones	9,4	10,3	8,1	11	27,1	31
Asesores de seguridad informática	5,5	5,8	6,3	7	20,5	23,2
Contratación de personal más calificado	1,8	1,8	2,0	3	13,9	11,3
Evaluaciones de seguridad internas y externas	9,9	9,8	9,6	4	25,9	25,1
Monitoreo de Seguridad Informática 7x24	-	-	-	-	25,3	25,6
Cursos especializados	-	-	-	-	-	25,6
Cursos de formación usuarios en seguridad informática	-	-	-	-	-	15,3
Pólizas de cibercriminal	-	-	-	-	-	4,43
Capacitación, auditoría, certificaciones de seguridad, continuidad del negocio	0,3	1,3	1,1	0	27,1	6,4

Fuente: Ibíd., p.47.

Los resultados obtenidos por los años 2007 y 2008, reafirman la inversión en seguridad de las redes de información, y un incremento poco significativo en el tema de control de la propiedad intelectual y derechos de autor.

La encuesta presenta un análisis de riesgos y vulnerabilidades a las que están expuestas las redes en general. Para estos riesgos, también actúan una serie de mecanismos que intervienen directamente en cada falla de seguridad. El estudio presenta unos resultados de los mismos, en los que se pueden destacar métodos efectivos y bastante utilizados como el cifrado de datos, contraseñas, antivirus, firewalls de Hardware y Firewalls de Software. Los resultados se presentan a continuación:

Tabla 37. Mecanismos de seguridad

	2002 %	2003%	2004 %	2005 %	2007	2008 %
Smart Cards	4	1,8	2,4	3	15	11,3
Biométricos (huella digital, iris, etc.)	2,1	1,9	1,6	2	18,4	19,7
Antivirus	0	17,6	16,2	14	86,4	76,4
Contraseñas	21,6	16,2	15,9	13	85	78,3
Cifrado de datos	10,2	7,8	7,7	7	39,5	42,9
Filtro de paquetes	7,4	5,6	6,3	7	34,7	28,1
Firewalls Hardware	8,8	8,5	8,5	8	55,1	49,3
Firewalls Software	8,6	11,1	11,5	12	66	58,1
Firmas digitales/ certificados digitales	3,3	4,4	3,5	' 5"	33,3	27,6
VPN / IPSec	7,2	5,5	5,5	7	44,2	51,2
Proxies	16,3	10,9	11,1	11	49,7	54,2
Sistemas de detec-ción de intrusos	6	5,3	5,9	7	29,9	27,1
Monitoreo 7x24	3,7	2,8	3,5	3	25,2	22,7

Fuente: Ibíd., p.53.

FECHA	25/11/2010

NÚMERO RAE	
PROGRAMA	INGENIERÍA DE SISTEMAS

AUTOR (ES)	CASTIBLANCO RIAÑO, Jorge; CARRILLO SANCHEZ, Jhonathan.
TÍTULO	DESARROLLO DE UN OBJETO VIRTUAL DE APRENDIZAJE (OVA) PARA EL DIAGNÓSTICO Y SEGUIMIENTO DE VULNERABILIDADES EN UNA RED INALÁMBRICA WI-FI

PALABRAS CLAVES	Redes inalámbricas Wi-Fi. Vulnerabilidades. Riesgos, seguridad. Objeto Virtual de Aprendizaje.

DESCRIPCIÓN	El objetivo de este proyecto es implementar un Objeto de Aprendizaje (OVA) para el diagnóstico y seguimiento de vulnerabilidades en redes inalámbricas WI-FI. La ventaja que ofrece esta nueva estrategia de aprendizaje, es la manera explícita del contenido publicado. Esto quiere decir que el alumno puede acceder a la información por medio de documentos, videos, imágenes, lecturas, opiniones y a su vez permite retroalimentar el sistema, para el uso posterior de dicho material.

FUENTES BIBLIOGRÁFICAS	ACIS, EVOLUCIÓN Y MONITOREO DE LA SEGURIDAD INFORMÁTICA, Revista: Sistemas No. 110, Abril – Junio 2009. ARIZA. Lina. Panorámica del Software Libre en Colombia. En: Sistemas. Septiembre-Noviembre, 2004, vol.90 CARRIER Brian D. IEEE SECURITY AND PRIVACY, Article: Digital Forensics work. Abril de 2009. CARRIER Brian D. IEEE SECURITY AND PRIVACY, Article: Security Education Using Second Life. Abril de 2009. GALLARDO Sara. "SISTEMAS: Gestión de la Inseguridad Informática, encuesta nacional. Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS). Bogotá D.C Colombia. Pág. 4-25. 2008 GALLARDO Sara. "SISTEMAS: Proyectos de Grado Ingeniería de Sistemas. Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS). Bogotá D.C Colombia. Pácanalg. 6-110. 2008 JACOBSON, Ivar; Booch, Grady; Rumbaugh James; El Proceso de Desarrollo de Software, Addison-Wesley, 1999. MASTER MAGAZINE Noviembre de 2007[En línea]. [Consulta: noviembre 2 de 2009]. [Def. Hardware]

Disponible en:*www.mastermagazine.info/termino/5330.php*

PICOUTO, Fernando. "Hacking y Seguridad en Internet" Alfa omega. Pág. 345-453. 2007

PRESSMAN S. Roger. Ingeniería del Software un enfoque práctico. México: Mc Graw Hill, 2006. 958

NÚMERO RAE	
PROGRAMA	INGENIERÍA DE SISTEMAS.

CONTENIDOS	**OBJETIVOS DE LA INVESTIGACIÓN** **Objetivo General:** desarrollar un Objeto Virtual de Aprendizaje (OVA) para el diagnóstico y seguimiento de vulnerabilidades en una red inalámbrica WI-FI, para facilitar el proceso de aprendizaje de los estudiantes, con el fin de adquirir la habilidad de prevenir incursiones no autorizadas a los sistemas de información y evitar posibles modificaciones o pérdidas de los datos. **Objetivos Específicos.** • Diseñar un OVA sobre seguridad en redes informáticas para facilitar el proceso de aprendizaje de los estudiantes. • Determinar la metodología para la implementación del OVA propuesto en el proyecto. • Desarrollar un Objeto Virtual de Aprendizaje, en el cual se especifiquen las principales características de la seguridad en las redes inalámbricas WI-FI. • Desarrollar pruebas funcionales y de aceptación del OVA, definidas en el diseño del software. **ALCANCES Y LIMITACIONES** **Alcances:** el desarrollo del Objeto Virtual de Aprendizaje (OVA), pretende orientar a los alumnos de la Universidad de San Buenaventura (Bogotá), en el área de diagnóstico y seguimiento de vulnerabilidades en redes inalámbricas.

La plataforma contará con una función de autenticación que permitirá el acceso a los usuarios registrados y de esta manera ingresar a su perfil y las herramientas disponibles en el OVA. La aplicación también permitirá la administración de archivos como videos, documentos, comentarios. Pdfs, e imágenes publicadas por los administradores y usuarios.

Limitaciones: la publicación del OVA se hará en un servidor que soporte Objetos virtuales de Aprendizaje. En caso de no localizar dicho espacio dentro de la Universidad de San Buenaventura se propone buscar un servidor externo.

Otra limitación es la capacidad que ofrezca el servidor en el que se aloje el Objeto virtual de aprendizaje, para la publicación de contenidos y archivos necesarios para la interacción de los usuarios.

METODOLOGÍA

ENFOQUE DE LA INVESTIGACIÓN

Empírico-analítico: el interés de este enfoque se caracteriza por interpretar y transformar objetos del mundo material. Por medio de la experimentación, se buscan medios más confiables, a la hora de solucionar un problema. Este enfoque permitirá implementar un Objeto Virtual de Aprendizaje para el diagnóstico y seguimiento de vulnerabilidades en redes inalámbricas para fines educativos y fortalecimiento del proceso de aprendizaje en alumnos de la Universidad San Buenaventura (Bogotá).

MARCO DE REFERENCIA

MARCO TEÓRICO CONCEPTUAL

El Objeto Virtual de Aprendizaje para el diagnóstico y seguimiento de vulnerabilidades en las redes Wi-Fi, tiene como objetivo general, la integración de conocimientos entre alumnos, docentes e investigadores. El OVA desarrollado es un aplicativo virtual de uso pedagógico, que permite la gestión de diversos tipos de archivos, para la comprensión de temas relacionados con la protección de la información en las organizaciones.

NÚMERO RAE	
PROGRAMA	INGENIERÍA DE SISTEMAS.
METODOLOGÍA	**LÍNEA DE INVESTIGACIÓN** **LÍNEA DE INVESTIGACIÓN DE LA UNIVERSIDAD DE SAN BUENAVENTURA SEDE BOGOTÁ.** Tecnologías actuales y sociedad. **SUB LÍNEA DE LA FACULTAD DE INGENIERÍA.** Sistemas de Información y Comunicación. **CAMPO DE INVESTIGACIÓN**. Desarrollo de Software y Redes de Computadores. **METODOLOGÍA DEL PROYECTO** Una metodología es un esquema de trabajo que permite estructurar, planificar y controlar el proceso de desarrollo de software. Por medio de una metodología se establecen las etapas que tendrá el proyecto para elaborar de forma ordenada y funcional cada ítem del software. El enfoque de la metodología es el modelo en cascada. Un modelo en cascada considera las principales actividades de especificación, desarrollo, validación y evolución del software y las divide en fases separadas. Las principales fases del modelo en cascada son: • **Análisis y definición de requerimientos:** esta etapa del modelo, permite identificar la funcionalidad del software mediante las especificaciones de los usuarios.

	• **Diseño**: permite establecer una arquitectura completa del sistema. El diseño identifica y describe las abstracciones fundamentales del software. • **Implementación:** el diseño del software es desarrollado mediante un conjunto de actividades y posteriormente implementadas para su funcionamiento. • **Pruebas:** permite la realización de pruebas para verificar el óptimo funcionamiento de los componentes del software.

CONCLUSIONES	Las nuevas tecnologías de información ofrecen herramientas y mecanismos que pueden fortalecer el proceso educativo de un alumno. El Objeto Virtual (OVA) fomenta el aprendizaje por medio de opiniones, documentos, videos, foros y comunidad, que permiten integrar diversos puntos de vista en el tema de diagnóstico y seguimiento de vulnerabilidades en redes inalámbricas Wi-Fi. La metodología utilizada en el desarrollo del OVA se caracteriza por tener una etapa de análisis, diseño, implementación y pruebas. Dicha metodología permitió establecer un orden o secuencia de pasos, para el desarrollo del software y la integración del Objeto Virtual de Aprendizaje para el diagnóstico y seguimiento de vulnerabilidades en redes Wi-Fi. Por medio del aplicativo (OVA) y el desarrollo de un simulador de las principales características de seguridad en una red Wi-Fi, se da a conocer a los alumnos las causas más conocidas de riesgos a las que están expuestas las redes informáticas y sus posibles soluciones. Conocer e identificar vulnerabilidades en las redes Wi-Fi, hace que se puedan adoptar contramedidas y establecer futuros vectores de ataque por parte de usuarios mal intencionados.