FACULTAD 4

Sistema informático para la detección de escaneos en Sistemas de Gestión de Contenidos Web

Trabajo de diploma para optar por el título de
Ingeniero en Ciencias Informáticas

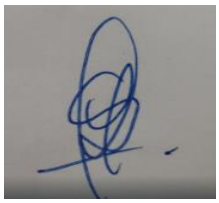
Autora: Yadira Sánchez Cruz
Tutores: P.A. M. Sc. Henry Raúl González Brito
P.A. M. Sc. Yadira Ramírez Rodríguez

La Habana, noviembre de 2023
"Año 65 de la Revolución"

DECLARACIÓN DE AUTORÍA

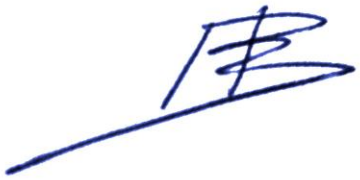
El autor del trabajo de diploma con título "***Sistema informático para la detección de escaneos en Sistemas de Gestión de Contenidos Web***", concede a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la investigación, con carácter exclusivo. De forma similar se declaran como únicos autores de su contenido. Para que así conste firman la presente a los 07 días del mes de noviembre del año 2023

Yadira Sánchez Cruz



Firma del Autor

Henry Raúl González Brito



Firma del Tutor

Yadira Ramírez Rodríguez

Firma del Tutor

DATOS DE CONTACTO

M. Sc. Henry Raúl González Brito: Ingeniero Informático por la Universidad de Camagüey y la Universidad Tecnológica de la Habana en el año 2005. Máster en Gestión de Proyectos Informáticos por la Universidad de Ciencias Informáticas en el año 2012 y Diplomado de Inteligencia Tecnológica en el año 2013. Profesor Auxiliar. Jefe de Departamento Docente de Ciberseguridad de la Facultad 2 y Coordinador del Colectivo de Carrera de Ingeniería en Ciberseguridad. Es secretario de la Comisión Nacional de Carrera Ingeniería en Ciberseguridad y miembro del Colectivo de Carrera del Programa de Formación del Nivel de Educación Superior de Ciclo Corto Administración de Redes y Seguridad Informáticas. Forma parte del claustro de la Maestría en Informática Avanzada, la Maestría en Calidad de Software, la Maestría en Informática Médica Aplicada y la Maestría en Telecomunicaciones y Telemática de la CUJAE, donde imparte posgrados en la temática de Ciberseguridad. Es Coordinador de la Especialidad de Posgrado en Seguridad Informática. Sus áreas de investigación están relacionadas con la seguridad en aplicaciones web, ciberseguridad y metodologías de pruebas de penetración. Es autor del libro "Administración Segura de Sistemas de Gestión de Contenidos Web", Ediciones Futuro, 2020, ISBN 978-959-286-078-0. Ha realizado diversas publicaciones y ponencias en eventos relacionadas con el campo de la ciberseguridad. Ha impartido cursos en eventos internacionales en Cuba y a estudiantes eslovacos, hondureños, colombianos, mexicanos y angoleños. Ha obtenido premios en el Fórum de Ciencia y Técnica y reconocimientos de las Brigadas Técnico Juveniles, incluyendo el Sello Forjadores del Futuro. Es miembro del Consejo Nacional de la Unión de Informáticos de Cuba y de su Consejo Técnico Asesor. Es integrante del Grupo de Ciberseguridad del Ministerio de Educación Superior y dirige del subcomité 27 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad del Comité Técnico de Normalización 18 del MINCOM. Es miembro del Consejo Científico de la Universidad de las Ciencias Informáticas.

Correo electrónico: henryraul@uci.cu.

M. Sc. Yadira Ramírez Rodríguez, graduada de Ingeniería en Ciencias Informáticas en el 2007. Máster en Calidad de Software y profesora auxiliar con más de 15 de años de experiencia en la asignatura de Ingeniería de Software. Jefa del Departamento Docente de Informática de la Facultad 4 de la Universidad de las Ciencias Informáticas. Líneas de Investigación: Ingeniería de Sistemas y Calidad de Software.

Correo electrónico: yramirezr@uci.cu

AGRADECIMIENTOS

A mis padres que han estado presentes siempre para mí, todo lo que soy hoy, es gracias a ellos y sus consejos, siendo ambos un ejemplo impecable tanto en el plano profesional como en el personal. Nunca encontrare suficientes palabras para agradecerles. A mi esposo, la persona que tanto amo, y que tantos planes hemos trazado, llegado este momento. A mi hermana, pues a pesar de la distancia, siempre ha estado incondicionalmente para apoyar y facilitar la realización de este proyecto. A mis amigos que siempre estuvieron presentes sin importar altas horas de la noche brindando opiniones y recomendaciones durante el desarrollo de la investigación. A mis tutores que han sabido guiarme correctamente y han sido ejemplo de profesionales para mí. A todas esas personas que formaron parte. Gracias. A la Universidad de las Ciencias Informáticas (UCI), que sin ella nada de esto hubiese ocurrido, por haberme permitido la preparación integral como profesional en Ciencias Informáticas.

A todos GRACIAS.

DEDICATORIA

A mis padres, mi esposo, mi hermana y a todos los que apoyaron en la obtención de este resultado que hoy se expone.

A todos GRACIAS.

RESUMEN

Las aplicaciones web son esenciales para la transformación digital en la sociedad actual, permitiendo la interacción entre personas y organizaciones en el ciberespacio. En Cuba, la informatización es una prioridad para el desarrollo económico y social, y la implementación de aplicaciones web ha mejorado la eficiencia y la transparencia en la gestión de los servicios públicos. Los sistemas de gestión de contenidos (CMS) son fundamentales para la creación de portales web, sin embargo, los CMS se han convertido en un objetivo atractivo para los ciberdelincuentes, y se han producido varios incidentes de ciberseguridad en los últimos años en CMS populares como WordPress, Drupal, Joomla y Magento. En Cuba, desde julio de 2021, se han intensificado los incidentes de ciberseguridad afectando la disponibilidad de varios sitios web gubernamentales, medios de prensa y organismos e instituciones. Para garantizar la ciberseguridad de los portales web basados en CMS, es necesario tomar medidas proactivas, y la detección de un ciberataque desde la fase del reconocimiento es crucial para bloquearlo desde el inicio. Sin embargo, existen deficiencias en la detección de escaneos en CMS debido a la cantidad de peticiones que se deben analizar, la ausencia de una base de datos con direcciones IP declaradas como atacantes y la necesidad de comprobar manualmente la presencia de direcciones IP sospechosas en bases de datos internacionales. El desarrollo de medios para la detección de escaneos en CMS es crucial para garantizar la ciberseguridad, especialmente en Cuba donde la informatización es una prioridad para su desarrollo económico y social.

PALABRAS CLAVE

Ciberseguridad, incidentes de ciberseguridad, sistemas de gestión de contenidos, Vulnerabilidad.

ABSTRACT

Web applications are essential for digital transformation in today's society, enabling interaction between people and organizations in cyberspace. In Cuba, computerization is a priority for economic and social development, and the implementation of web applications has improved efficiency and transparency in the management of public services. Content management systems (CMS) are central to the creation of web portals, however, CMSs have become an attractive target for cybercriminals, and several cybersecurity incidents have occurred in recent years in popular CMSs such as WordPress, Drupal, Joomla, and Magento. In Cuba, since July 2021, cybersecurity incidents have intensified, affecting the availability of several government websites, press outlets and agencies and institutions. To ensure the cybersecurity of CMS-based web portals, proactive measures need to be taken, and detecting a cyberattack from the recognition phase is crucial to block it from the start. However, there are shortcomings in the detection of scans in CMS due to the number of requests that must be analyzed, the absence of a database with IP addresses declared as attackers and the need to manually check the presence of suspicious IP addresses in international databases. The development of means for the detection of scans in CMS is crucial to guarantee cybersecurity, especially in Cuba where computerization is a priority for its economic and social development.

KEYWORDS

Cybersecurity, cybersecurity incidents, content management systems, vulnerability.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

OPINIÓN DEL(OS) TUTOR(ES)

<Contenido de la opinión de los tutores>

AVAL DEL CLIENTE

<Contenido del aval del cliente sobre la solución desarrollada

INTRODUCCIÓN

Las aplicaciones web son fundamentales para la transformación digital de la sociedad actual. La interacción entre personas y organizaciones se lleva a cabo en gran medida en el ciberespacio a través de estas aplicaciones. Los usuarios pueden acceder a la web mediante navegadores como Firefox o Chrome, así como, a través de aplicaciones móviles nativas que presentan los contenidos de manera óptima para estos dispositivos. En la actualidad, cualquier organización, empresa o entidad que desee tener presencia en línea debe tener un portal web.

La informatización es una prioridad en Cuba, y se ha convertido en una herramienta clave para el desarrollo económico y social del país. La implementación de aplicaciones web en Cuba ha permitido la creación de servicios en línea para la gestión de trámites, como el pago de impuestos, la solicitud de visas y la consulta de información médica. Además, ha facilitado la comunicación entre las empresas y el gobierno, lo que ha mejorado la eficiencia y la transparencia en la gestión de los servicios públicos.

Los portales web también son importantes para el desarrollo de la educación en Cuba, ya que permiten el acceso a la información y los recursos educativos en línea, lo que facilita el aprendizaje y la formación continua. Esto se vio reflejado durante la pandemia de COVID-19 cuando se utilizaron de forma masiva plataformas basadas en Moodle para la continuación de la formación de los estudiantes en modalidad a distancia.

Para la creación de portales web, una de las herramientas más utilizadas en la actualidad son los Sistemas de Gestión de Contenidos o CMS (por sus siglas en inglés), las cuales constituyen herramientas que permiten a los usuarios crear, editar, publicar y gestionar contenido en línea de manera eficiente y sencilla como por ejemplo sitios web, blogs, tiendas en línea, foros, entre otras aplicaciones. Están diseñados para ser fáciles de usar y no requieren conocimientos de programación para crear contenidos o actualizarlos. Los contenidos creados además pueden ser publicados en múltiples plataformas, lo que ahorra tiempo y reduce la duplicación de esfuerzos. Su facilidad de uso, eficiencia, flexibilidad y capacidad de colaboración ha hecho posible que por ejemplo el CMS WordPress representa, según W3Techs el 64.1% de todos los sitios web publicados en Internet. Por este motivo, no es de extrañar que la popularidad de los CMS los convierta en un objetivo atractivo para los ciberdelincuentes. A continuación, se mencionan algunos de los principales incidentes de ciberseguridad que han afectado a los CMS en los últimos años:

- Ataque a WordPress en 2020: En septiembre de 2020, se descubrió un ataque masivo de fuerza bruta en los sitios web de WordPress. Los atacantes intentaron acceder a las cuentas de administrador mediante la prueba de diferentes combinaciones de nombre de usuario y contraseña. Se informó que la campaña afectó a más de 1 millón de sitios web de WordPress en todo el mundo.
- Vulnerabilidad en Magento en 2019: En febrero de 2019, se descubrió una vulnerabilidad crítica en Magento que permitía a los atacantes tomar el control de los sitios web afectados. La vulnerabilidad afectó a todas las versiones de Magento desde la versión 2.0.0 hasta la versión 2.3.0.
- Vulnerabilidad en Drupal en 2018: En marzo de 2018, se descubrió una vulnerabilidad crítica en Drupal que permitía a los atacantes ejecutar código malicioso en los sitios web afectados. La vulnerabilidad afectó a todas las versiones de Drupal desde la versión 6 hasta la versión 8.4.7.
- Ataque a Joomla en 2017: En agosto de 2017, se descubrió un ataque masivo de inyección de SQL en los sitios web de Joomla. Los atacantes explotaron una vulnerabilidad en la extensión JCE Editor de Joomla para acceder a las bases de datos de los sitios web afectados. Se informó que el ataque afectó a más de 2,5 millones de sitios web de Joomla en todo el mundo.
- Ataque a WordPress en 2017: En abril de 2017, se descubrió un botnet que se estaba utilizando para atacar los sitios web de WordPress. Los atacantes aprovecharon una vulnerabilidad en la extensión REST API de WordPress para ejecutar ataques de fuerza bruta y tomar el control de los sitios web afectados. Se informó que el botnet afectó a más de 1,5 millones de sitios web de WordPress en todo el mundo.

Los incidentes antes mencionados son solo una parte de la gran cantidad de problemas de seguridad que ocurren diariamente en Internet con este tipo de tecnología, por lo que es necesario tomar medidas proactivas para garantizar la protección de los portales web basados en CMS contra posibles vulnerabilidades y ciberataques. Cuba no ha estado ajena a estos problemas pues los portales web son fundamentales para la informatización en Cuba, ya que permiten el acceso a la información y los servicios en línea, lo que facilita la comunicación y el intercambio de información entre personas, empresas y organizaciones. Desde el 12 de julio de 2021 y hasta la fecha, se intensificó la ocurrencia de incidentes de ciberseguridad, que han afectado la disponibilidad de varios sitios web gubernamentales entre ellos el de la Presidencia de Cuba, y el del Ministerio de Relaciones

Exteriores. También han sido atacados los pertenecientes a medios de prensa nacionales como los portales del periódico Granma y Cubadebate, así como los de varios organismos e instituciones.

Para que un ciberataque tenga éxito, debe pasar por una serie de fases que han sido conceptualizadas en el modelo Cyber KillChain, (ver figura 1). Este modelo explica que, si una de esas fases es bloqueada por los defensores, el ciberataque se interrumpe y los adversarios no podrán alcanzar sus objetivos.

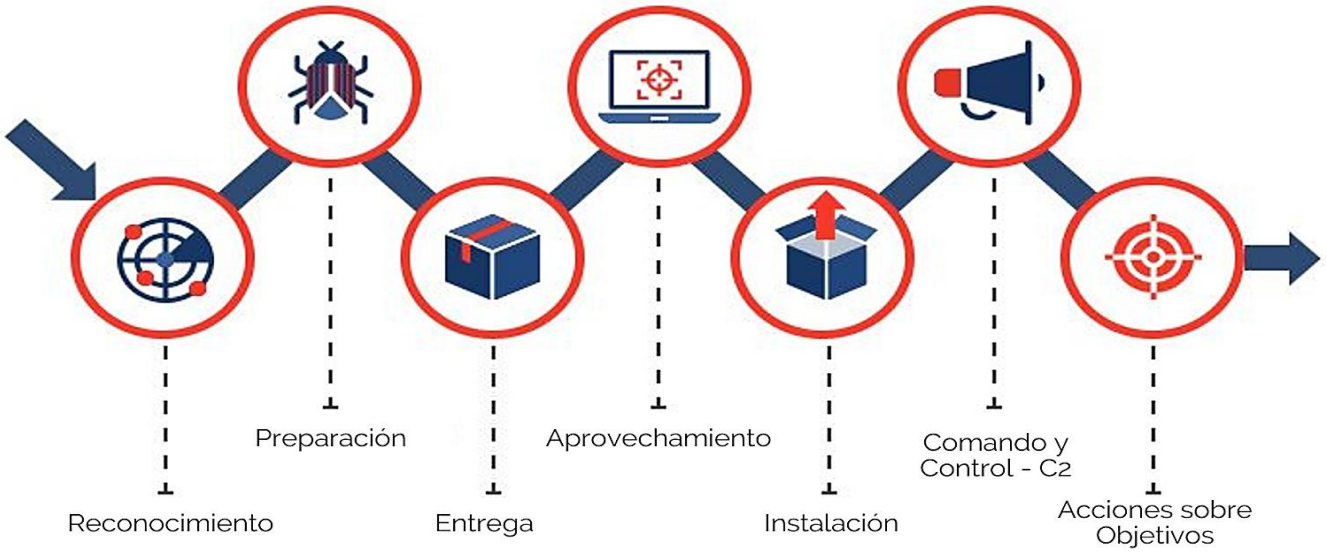


Figura 1 Modelo Cyber KillChain

La primera fase en los ataques es el reconocimiento, donde se usan técnicas basadas en escaneos para comprender las tecnologías y características del blanco. La detección de un ciberataque desde la fase del reconocimiento, permitiría bloquearlo desde el inicio, contribuyendo a garantizar la ciberseguridad del portal web. Los CMS, al estar constituidos por elementos comunes (componentes, temas y recursos estándares) permiten detectar patrones de escaneos con más facilidad que los portales hechos con otras tecnologías, no obstante, existen una serie de deficiencias que dificultan la puesta en práctica del proceso de detección de los escaneos:

- Los especialistas de seguridad deben comprobar manualmente si desde una dirección IP están escaneando la presencia de determinados recursos asociados al despliegue de un CMS, aspecto que se dificulta por la cantidad de peticiones que se deben analizar, las cuales pueden alcanzar la cifra de decenas de miles.
- La ausencia de una base de datos con direcciones IP declaradas como atacantes dificulta la comprobación de un historial de reputación que facilite la identificación rápida de direcciones

IP adversarias, pues es muy probable que una dirección IP se utilice para la realización de ataques de tipo escaneo contra otros portales web. Esta cuestión también dificulta el suministro de información útil a los mecanismos de seguridad tecnológica como cortafuegos y sistemas de detección de intrusiones.

- Para una investigación más profunda, es necesario también comprobar manualmente la presencia de las direcciones IP sospechosas en bases de datos internacionales de direcciones IP comprometidas, este proceso es lento pues por lo general deben comprobarse decenas de direcciones de IP al día.

Todo lo analizado hasta el momento evidencia la importancia que tiene el desarrollo de los medios para la detección de escaneos en sistemas de gestión de contenidos web planteándose como **problema de investigación** ¿Cómo contribuir a elevar la seguridad de los Sistemas de Gestión de Contenidos Web? Teniendo como **objeto de estudio** Proceso para la detección de escaneos en Sistemas de Gestión de Contenidos Web, enfocándose en la detección de escaneos en Sistemas de Gestión de Contenidos Web como **Campo de acción**. Teniendo como **objetivo general** desarrollar un sistema informático para la detección de escaneos que contribuya a elevar la seguridad de los Sistemas de Gestión de Contenidos Web, enfocándose en las siguientes tareas:

Tareas de Investigación

1) Sistematización de los principales fundamentos teóricos y metodológicos a nivel nacional e internacional para el desarrollo de un sistema informático que facilite la detección de escaneos en Sistemas de Gestión de Contenidos Web
2) Diagnóstico del estado actual del proceso detección de escaneos en Sistemas de Gestión de Contenidos Web
3) Implementación de un sistema informático que contribuya a elevar la seguridad de los Sistemas de Gestión de Contenidos Web
4) Validación del sistema informático para resolver el problema de investigación desarrollado.

Para el desarrollo de la investigación se emplean los siguientes métodos científicos:

Métodos teóricos:

- Método analítico-sintético: para analizar desde diferentes aristas los conceptos asociados a la gestión de IP sospechosas y sintetizar los datos recopilados. Este procedimiento permite

describir y precisar las características generales a tener en cuenta y establecer los principales elementos de las peticiones e incidentes de seguridad.

- Inductivo-deductivo: Se emplea principalmente para la elaboración del marco teórico de la investigación de manera que se pueda ir de lo general a lo particular precisando los elementos fundamentales del objeto de estudio y del campo de acción
- Histórico-lógico: Para determinar las tendencias actuales de los sistemas para la gestión de IP maliciosas, de los modelos de desarrollo y las técnicas, lenguajes y herramientas utilizadas durante la investigación.
- Modelación: Este método permite reflejar la estructura, relaciones internas y características de la solución a través de diagramas.

Métodos empíricos:

- Observación: se lleva a cabo para el proceso de gestión de IP sospechosas, .se observaron los elementos que la componen y como se gestionan.

El presente trabajo de diploma, está compuesto por tres capítulos, que incluyen los procedimientos desarrollados en relación con el trabajo investigativo, así como la propuesta de solución y validación de la investigación.

Capítulo 1 - Fundamentación Teórica: en esta primera etapa se abordó el estado del arte del tema que se investiga. Se destaca un estudio bibliográfico detallado sobre los principales conceptos asociados a las peticiones e incidentes de ciberseguridad. En el transcurso de esta etapa, mientras se realizó el análisis del objeto de investigación, se seleccionaron las tecnologías de desarrollo acordes para incorporar estas prestaciones en el sistema desarrollado. Se describió el objeto de estudio y el campo de acción de la investigación.

• Capítulo 2 - Características y diseño del sistema: se describió el procedimiento seguido en las etapas de planificación y diseño que propone la metodología XP. Se especificaron las Historias de Usuarios (HU), el plan de iteraciones y el plan de entregas. También se describió la propuesta de solución y se mencionaron los patrones de diseño utilizados en la implementación de los módulos.

• Capítulo 3 - Implementación y prueba del sistema: en esta etapa se definieron las tareas de ingenierías correspondientes a cada HU. También se aplicaron las pruebas de aceptación que permitieron comprobar el correcto funcionamiento de las funcionalidades implementadas

CAPÍTULO I: FUNDAMENTOS Y REFERENTES TEÓRICO-METODOLÓGICOS SOBRE EL OBJETO DE ESTUDIO

En este capítulo se abordan los aspectos fundamentales que servirán de soporte teórico para el desarrollo de la investigación, dígase, fundamentación teórica, donde se describen las características que debe tener un sistema informático, teniendo en cuenta los procesos de gestión de IP sospechosas. Incluye además un análisis del estado actual de los sistemas informáticos más utilizados para la gestión IP sospechosas. Además, se justifica la elección de la metodología, lenguajes, herramientas y tecnologías a utilizar para el desarrollo de la propuesta de solución.

1.1 Proceso para la detección de escaneos en CMS

Cuando se habla de proceso de detección de escaneo en los CMS se refiere a la identificación de patrones de ataque dirigidos a los CMS más populares, como WordPress, Joomla y Drupal (Jana y Oprea, 2019; Kasturi et al., 2020). Los atacantes pueden utilizar herramientas de escaneo automatizadas para buscar sitios web que utilicen estos CMS y, a continuación, intentar encontrar vulnerabilidades conocidas en las versiones del CMS instaladas (Jagamogan, Ismail, Hafizah, y Abas, 2021). Este proceso consta de 5 actividades fundamentales:

- **Recopilación de registros de actividad**: Consiste en recopilar los registros de actividad del CMS. Estos registros incluyen información sobre las solicitudes entrantes al sistema, como direcciones IP de origen, URLs solicitadas y otra información relevante.
- **Análisis de patrones de actividad**: Consiste en analizar los patrones de actividad en los registros recopilados. Esto implica buscar comportamientos sospechosos que indiquen posibles escaneos automáticos o intentos de exploración en el CMS. Se pueden utilizar técnicas de análisis de datos, como el análisis de frecuencia y el reconocimiento de patrones, para identificar anomalías.
- **Uso de listas negras**: Una estrategia común es utilizar listas negras de direcciones IP conocidas por realizar escaneos o actividades maliciosas. Estas listas se actualizan regularmente y se comparan con las direcciones IP en los registros de actividad del CMS. Si se encuentra una coincidencia, se considera sospechosa y se toman medidas adicionales.
- **Implementación de sistemas de detección de intrusiones (IDS)**: Los IDS pueden utilizar firmas y algoritmos para detectar patrones específicos que indiquen escaneos en el CMS. Estos sistemas pueden monitorear el tráfico entrante y compararlo con patrones conocidos de

escaneo. Si se detecta una coincidencia, se generan alertas o se toman medidas automatizadas.

- **Investigación y respuesta:** Si se identifica una actividad sospechosa de escaneo, es importante realizar una investigación adicional y responder de manera adecuada. Esto puede implicar la recopilación de más información sobre la fuente del escaneo, la identificación de posibles vulnerabilidades en el CMS y la adopción de medidas correctivas.

Cuando se habla de la identificación de patrones de ataque es necesario conocer que según el Decreto 360 de la República de Cuba referente a la seguridad de las tecnologías de la información y la comunicación y la defensa del ciberespacio nacional denomina ataque al intento de acceso o acceso a un sistema o una red informática o terminal mediante la explotación de vulnerabilidades existentes en su seguridad. Se identifica como riesgo a la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático y cause un impacto negativo en la organización (Consejo_de_Ministros, 2019). Como se explica en el modelo Cyber Kill Chain (Naik, Jenkins, Grace, y Song, 2022), el primer paso de un ciberataque es el proceso de reconocimiento donde el atacante identifica el objetivo y recopila información sobre el mismo, incluyendo técnicas de escaneo de vulnerabilidades.

Las vulnerabilidades son errores, fallas, debilidades o exposiciones internas de una aplicación, dispositivo del sistema o servicio que podría conducir a un error de confidencialidad, integridad o disponibilidad (Franklin, Wergin, y Booth, 2014). Algunas de las principales vulnerabilidades web son (González Brito y Montesino Perurena, 2018; Humayun et al., 2020; Lala, Kumar, y Subbulakshmi, 2021):

- **Inyección de código**: Las vulnerabilidades de inyección de código SQL, HTML, OS, PHP y otros, ocurren cuando la aplicación no está preparada para validar y detectar códigos dañinos que puede ser insertado como parte de una secuencia de datos legítima(Dong et al., 2018).
- **Pérdida de Autenticación y Gestión de Sesiones**: Las funciones de la aplicación relacionadas con la autenticación y gestión de sesiones son implementadas de forma incorrecta, lo que posibilita que los ciberatacantes puedan explotar fallas que les permitan tomar la identidad de los usuarios (Calzavara, Focardi, Squarcina, y Tempesta, 2017; González Brito y Montesino Perurena, 2018).
- **Secuencia de Comandos en Sitios Cruzados (XSS)**: Las fallas XSS ocurren cuando una aplicación envía datos no confiables al navegador web sin una validación y codificación apropiada (Wang, Xu, Zeng, Li, y Feng, 2017).

- **Control de Acceso Interrumpido**: Las restricciones a las funciones que los usuarios tienen permiso para utilizar no se cumplen correctamente. Dentro de este grupo de vulnerabilidades se destacan:
    - **Referencia Directa Insegura a Objetos**: Ocurre cuando un desarrollador expone una referencia a un objeto interno, como un archivo, directorio, o base de datos y no hay un chequeo de control de acceso efectivo.
    - **Ausencia de Control de Acceso a Funciones**: Las aplicaciones web no verifican los permisos de acceso a nivel de función antes de mostrarlas en la interfaz de usuario.
    - **Configuración de Seguridad Incorrecta**: No se aplican adecuadamente las configuraciones de seguridad propuestas para las aplicaciones, marcos de trabajo, bases de datos, servidores web y sistemas operativos (Akiyama, Yagi, Yada, Mori, y Kadobayashi, 2017).
    - **Exposición de datos sensibles**: Está provocado por las deficiencias en la protección adecuada de datos sensibles tales como credenciales de cuentas de usuarios, números de tarjetas de crédito y otros datos personales (Mansfield-Devine, 2017).
- **Falsificación de peticiones en sitios cruzados (CSRF)**: Esta vulnerabilidad permite que los ciberatacantes puedan obligar al navegador de un usuario autenticado a enviar una petición HTTP manipulada sin conocimiento de este (Martínez, Cosentino, y Cabot, 2017).
- **Utilización de componentes con vulnerabilidades conocidas**: Está dado por la utilización de componentes (librerías, marcos de trabajos, extensiones y otros módulos) con vulnerabilidades conocidas, que debilitan la defensas y amplían la superficie de ataque (Morrison, Smith, y Williams, 2017).
- **Entidades externas de XML (XXE)**: Las entidades externas en documentos XML pueden utilizarse para revelar archivos en servidores no actualizados, escaneo de puertos, ejecución de código, entre otros.
- **Deserialización insegura**: Ocurre cuando una aplicación recibe objetos serializados manipulados para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución (Seacord, 2017).
- **Registro y monitoreo insuficiente**: El deficiente monitoreo de los registros de operación de las aplicaciones web permiten a los ciberatacantes vulnerar los controles de seguridad (Shugrue, 2017).

Como puede observarse en la figura 2, las vulnerabilidades web representan un gran riesgo de seguridad para el funcionamiento adecuado de las aplicaciones web. Por ello es muy importante

establecer medidas proactivas que limiten su presencia y eviten su explotación por los atacantes. Dentro de estas medidas proactivas está la detección de escaneos web por parte de los atacantes.

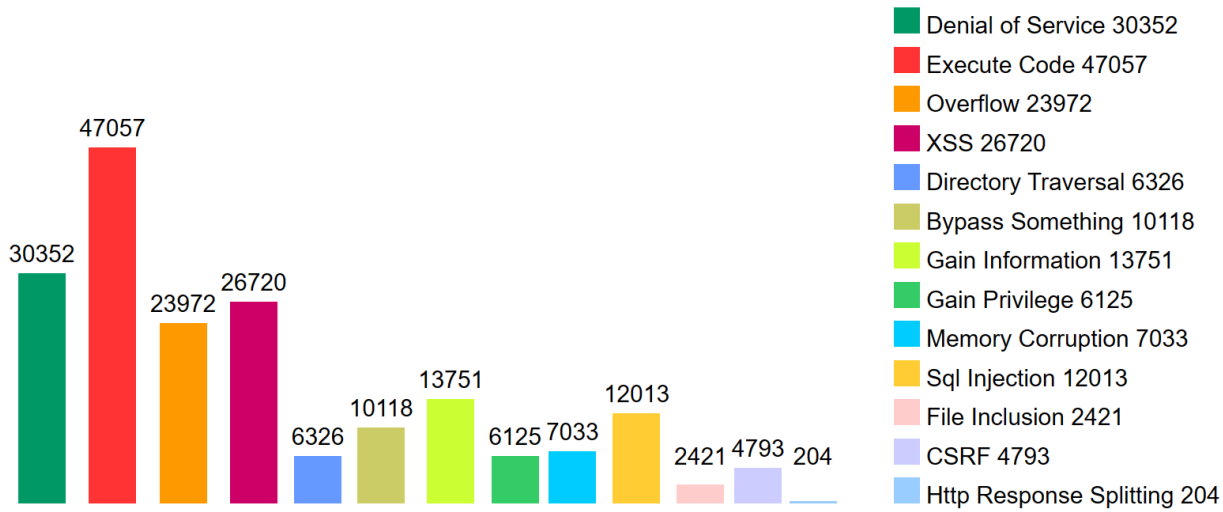


Figura 2. Distribución de vulnerabilidades por tipo. Tomado de CVEDetails.com

1.2 La detección de escaneos en CMS

El objetivo principal de detectar los ataques de escaneos web es proteger los sistemas y aplicaciones web contra posibles ataques. La detección temprana de los escaneos web puede ayudar a los propietarios de los sitios web a identificar y mitigar las posibles vulnerabilidades antes de que sean explotadas por los atacantes, así como bloquear las direcciones IP que están realizando este ataque, de este modo se pueden aplicar medidas proactivas para evitar que los atacantes accedan a los sistemas (Kozik, Choraś, Renk, y Hołubowicz, 2014; Y. Li y Q. Liu, 2021).

Se debe tener presente que un ataque de escaneo es un tipo de ataque informático que se utiliza para identificar vulnerabilidades en un sistema o red. El atacante utiliza herramientas automatizadas o manuales para enviar una serie de paquetes de datos a través de la red, con el objetivo de identificar dispositivos, servicios o puertos abiertos en el sistema objetivo (Kissel, 2019; Patel, 2019; Woo, Jang, y Kang, 2021). El objetivo del ataque de escaneo es recopilar información sobre el sistema objetivo, como la arquitectura del sistema, los servicios y aplicaciones que se están ejecutando, los puertos abiertos y cualquier otra información que pueda ser utilizada para identificar vulnerabilidades y debilidades en el sistema (Dhanya et al., 2023).

Una vez que el atacante ha identificado las vulnerabilidades, puede intentar explotarlas para obtener acceso no autorizado al sistema o red (Ahlawat, Tudu, Gaur, Fujita, y Singh, 2019). Por ejemplo, un atacante podría utilizar un escaneo de puertos para identificar un puerto abierto que esté utilizando un protocolo de comunicación débil o vulnerable, y luego utilizar esa información para llevar a cabo

ataques de inyección de código, ataques de denegación de servicio, robo de datos o instalación de malware. Estos ataques pueden tener graves consecuencias para la organización, incluyendo la pérdida de datos, la interrupción de los servicios, la pérdida de la reputación y la responsabilidad legal (Jang, Woo, Kim, y Kang, 2021; Kumar y Lim, 2019).

Para protegerse contra los ataques de escaneo, es importante implementar medidas de seguridad adecuadas, como el uso de firewalls, la implementación de políticas de seguridad robustas, la actualización de software y firmware de manera regular y la realización de pruebas regulares de penetración para identificar y corregir las vulnerabilidades (Huang, Zhang, Cheng, y Shieh, 2017; Mazurczyk y Caviglione, 2021).

En el Artículo 88 del Decreto 360 de la República de Cuba se expresa que solo "la entidad autorizada es la única que puede explorar o monitorear las redes públicas de transmisión de datos, en busca de vulnerabilidades o información sobre sus usuarios" (Consejo_de_Ministros, 2019), esto quiere decir que los escaneos se consideran también en el contexto cubano como parte de las acciones ofensivas si no se desarrollan por entidades autorizadas y que por tanto deben ser detectadas y combatidos.

Por otra parte, un escaneo web es un proceso automatizado que se utiliza para identificar vulnerabilidades en un sitio web. Los atacantes pueden realizar escaneos web para descubrir posibles vulnerabilidades en un sitio web, con el fin de explotarlas y comprometer la seguridad del sitio web. Existen diferentes tipos de escaneos web, algunos de los cuales son (Saputra, Utami, y Muhammad, 2022; Shahid et al., 2022):

- **Escaneo de puertos**: Este tipo de escaneo se utiliza para identificar los puertos abiertos en el servidor web y los servicios que se están ejecutando en ellos.
- **Escaneo de vulnerabilidades**: Este tipo de escaneo se utiliza para identificar vulnerabilidades específicas en el servidor web. Los atacantes pueden utilizar herramientas de escaneo de vulnerabilidades automatizadas, como Nessus o OpenVAS, para realizar este tipo de escaneo.
- **Escaneo de fuerza bruta**: Este tipo de escaneo se utiliza para identificar credenciales débiles o predecibles en una aplicación web. Los atacantes pueden utilizar herramientas automatizadas, como Hydra o Medusa, para realizar este tipo de escaneo.

Los atacantes pueden utilizar diferentes técnicas para realizar un escaneo web, como el uso de herramientas automatizadas, como Nmap o Nikto, o el uso de scripts personalizados que se ejecutan en un navegador web. Estas técnicas pueden ayudar a los atacantes a identificar vulnerabilidades en un sitio web y a realizar ataques exitosos. Por ello es tan importante detectarlos a tiempo para impedir que el ataque escale a fases más avanzadas (Mazurczyk y Caviglione, 2021).

La detección de un escaneo web presenta diversas dificultades, ya que los atacantes pueden utilizar diferentes técnicas para ocultar su actividad y evitar ser detectados (Mazurczyk y Caviglione, 2021). Sin embargo, hay algunas señales de alerta que pueden indicar que un escaneo web está en curso. Algunos de estos indicadores son:

1. **Tráfico de red inusual**: Un escaneo web puede generar un gran volumen de tráfico de red que puede ser detectado por herramientas de monitoreo de red como Wireshark o tcpdump. Los patrones de tráfico de red inusual, como un gran número de solicitudes a un solo puerto o una sola dirección IP, pueden indicar la presencia de un escaneo web (Kim, Park, y Lee, 2020).
2. **Registros del servidor web**: Los registros del servidor web pueden revelar patrones de actividad inusual, como un gran número de solicitudes de un solo usuario o una sola dirección IP. Estos registros pueden ser analizados para detectar patrones de actividad malintencionada (Sureda Riera, Bermejo Higuera, Bermejo Higuera, Martínez Herraiz, y Sicilia Montalvo, 2020).
3. **Alertas de seguridad**: Las soluciones de seguridad como los firewalls y los sistemas de detección de intrusiones pueden generar alertas cuando se detectan patrones de actividad malintencionada. Por ejemplo, un firewall puede generar una alerta cuando se detectan muchas solicitudes a un solo puerto en un corto período de tiempo (Yuan et al., 2019).
4. **Herramientas de detección de escaneo**: Existen herramientas específicas de detección de escaneo web, como Fail2ban o Snort, que pueden analizar el tráfico de red y detectar patrones de actividad malintencionada (Dawamsyach, Ruslianto, y Ristian).

Es importante tener en cuenta que, aunque estos indicadores pueden ayudar a detectar un escaneo web, no son infalibles. Los atacantes pueden utilizar técnicas avanzadas para evitar ser detectados, por lo que es importante mantenerse alerta y tomar medidas de seguridad adecuadas para proteger los sistemas y aplicaciones web.

Bloquear las direcciones IP de los atacantes es una medida de seguridad efectiva que ayuda a proteger los sistemas y aplicaciones web contra posibles ataques. Cuando se detecta actividad malintencionada en una dirección IP específica, bloquear esa dirección IP puede ayudar a prevenir futuros intentos de ataque desde esa dirección IP. Con ello se pueden lograr los siguientes beneficios (Špaček, Laštovička, Horák, y Plesník, 2019; Wickramasinghe, Nabeel, Thilakaratne, Keppitiyagama, y De Zoysa, 2021) :

- **Prevenir ataques futuros**: Bloquear las direcciones IP de los atacantes puede ayudar a prevenir futuros intentos de ataque desde esas direcciones IP específicas. Esto puede ayudar

a reducir la exposición a posibles ataques y mejorar la seguridad de los sistemas y aplicaciones web.

- **Ahorrar recursos**: Al bloquear las direcciones IP de los atacantes, se pueden ahorrar recursos valiosos del sistema y de la red que de otro modo se utilizarían para responder a los intentos de ataque. Esto puede ayudar a mejorar el rendimiento de los sistemas y reducir los costos asociados con la gestión de la seguridad.
- **Proteger la privacidad de los usuarios**: Al bloquear las direcciones IP de los atacantes, se pueden proteger la privacidad y la seguridad de los usuarios de los sistemas y aplicaciones web. Los atacantes pueden intentar acceder a información confidencial de los usuarios, como nombres de usuario, contraseñas y otra información personal, por lo que bloquear las direcciones IP de los atacantes puede ayudar a prevenir la exposición de esta información.

Hay varias formas de bloquear direcciones IP específicas en un sitio web, dependiendo del servidor web y del sistema operativo que esté utilizando. Algunas de las formas más comunes de bloquear direcciones IP son:

- **Utilizando un firewall**: La mayoría de los servidores web tienen un firewall integrado que puede utilizarse para bloquear direcciones IP específicas. Por ejemplo, si está utilizando el servidor web Apache, puede agregar reglas de firewall utilizando el módulo mod_security.
- **Utilizando un archivo .htaccess**: Si está utilizando el servidor web Apache, puede bloquear direcciones IP específicas utilizando el archivo .htaccess. Para hacerlo, simplemente agregue las direcciones IP que desea bloquear en el archivo .htaccess.
- **Utilizando un software de seguridad**: Hay varios softwares de seguridad que pueden utilizarse para bloquear direcciones IP específicas en un sitio web. Por ejemplo, el software de seguridad ModSecurity puede utilizarse para bloquear direcciones IP específicas en un sitio web.
- **Utilizando un complemento del CMS**: Por ejemplo, si se está utilizando el CMS WordPress, hay varios plugins que pueden utilizarse para bloquear direcciones IP específicas. (Špaček, Laštovička, Horák, y Plesník, 2019; Wickramasinghe, Nabeel, Thilakaratne, Keppitiyagama, y De Zoysa, 2021)

Bloquear direcciones IP específicas puede ser una medida efectiva para proteger un sitio web contra posibles ataques, pero también puede tener algunos riesgos asociados. Algunos de los principales riesgos de bloquear direcciones IP son:

- **Bloquear a usuarios legítimos**: Si se bloquean direcciones IP sin tener en cuenta el contexto y la naturaleza de la actividad, es posible que se bloqueen a usuarios legítimos que estén intentando acceder al sitio web. Esto puede resultar en una mala experiencia del usuario y en la pérdida de clientes o visitantes.
- **Falsos positivos**: Es posible que se identifiquen direcciones IP como malintencionadas cuando en realidad son legítimas, lo que podría resultar en falsos positivos. Esto puede hacer que se bloquee el acceso a usuarios legítimos y resultar en la pérdida de clientes o visitantes.
- **Evasión de medidas de seguridad**: Los atacantes pueden utilizar técnicas para evitar ser detectados y bloqueados a través de sus direcciones IP. Por ejemplo, pueden utilizar direcciones IP de proxy o cambiar frecuentemente de dirección IP para evitar ser bloqueados.
- **Pérdida de información valiosa**: Si se bloquean direcciones IP sin tener en cuenta el contexto y la naturaleza de la actividad, es posible que se pierda información valiosa sobre los atacantes y sus técnicas. Esto puede dificultar la identificación y mitigación de futuros intentos de ataque (Špaček, Laštovička, Horák, y Plesník, 2019; Wickramasinghe, Nabeel, Thilakaratne, Keppitiyagama, y De Zoysa, 2021).

1.3 Soluciones informáticas para Detección de Escaneos en CMS

Existen diferentes tecnologías para la detección de escaneos en sistemas de gestión de contenidos web. Estos pueden clasificarse del siguiente modo:

Sistemas de Detección de Intrusiones a nivel de Red

Un sistema de detección de intrusiones a nivel de red (en inglés: Network Intrusion Detection System o NIDS) es una herramienta de seguridad informática que monitorea el tráfico de red en tiempo real para detectar posibles ataques y actividades maliciosas. El objetivo de un NIDS es identificar patrones sospechosos en el tráfico de red, como intentos de acceso no autorizado, actividad de virus y malware, ataques de denegación de servicio, escaneo de puertos, entre otros (Thakkar y Lohiya, 2022).

Para lograr esto, un NIDS utiliza técnicas de análisis de tráfico de red, como la inspección de paquetes y la comparación de patrones, para detectar actividades maliciosas y generar alertas en caso de que se detecte alguna actividad sospechosa. Los NIDS pueden ser implementados de

manera distribuida en la red, en diferentes puntos de acceso, para aumentar su eficacia y cubrir todo el tráfico de la red. También pueden ser configurados para tomar medidas proactivas, como bloquear el tráfico sospechoso o alertar a los administradores de seguridad para que tomen medidas (Ahmad, Shahid Khan, Wai Shiang, Abdullah, y Ahmad, 2021).

Sistemas de Detección de Intrusiones a nivel de Host

Un sistema de detección de intrusiones a nivel de host (en inglés: Host Intrusion Detection System o HIDS) es una herramienta de seguridad informática que se instala en un host o servidor individual para monitorear y detectar posibles intrusiones o actividades maliciosas en ese host específico (Bridges, Glass-Vanderlan, Iannacone, Vincent, y Chen, 2019).

El objetivo de un HIDS es detectar actividades sospechosas en el nivel del host, como cambios no autorizados en archivos del sistema, intentos de acceso no autorizado a cuentas de usuario, modificaciones en configuraciones críticas del sistema operativo, entre otros. Para lograr esto, un HIDS utiliza técnicas de análisis de sistema, como la monitorización de archivos, la verificación de integridad del sistema operativo y la detección de procesos maliciosos activos, para detectar cualquier actividad sospechosa (Soliman, Sobh, y Bahaa-Eldin, 2021).

Los HIDS a menudo están diseñados para ser más específicos que los NIDS, ya que se centran en la protección de un solo host en lugar de la red completa. Además, los HIDS pueden ser configurados para tomar medidas proactivas, como bloquear el tráfico sospechoso o alertar a los administradores de seguridad para que tomen medidas. En general, los HIDS son una herramienta importante en la protección de sistemas individuales contra posibles intrusiones y actividades maliciosas (Nair y Mhavan, 2023).

Listas Negras (Blacklist)

Las blacklists (listas negras, en español) son listas de direcciones IP, nombres de dominio o direcciones de correo electrónico que se consideran maliciosas o sospechosas por diversos motivos, y que se utilizan para bloquear el acceso a estos recursos por parte de sistemas o usuarios que los intentan utilizar (Nair y Mhavan, 2023). Las blacklists se utilizan en diferentes contextos, como, por ejemplo, para bloquear el acceso a sitios web maliciosos o para prevenir el spam en correos electrónicos. Estas listas se actualizan continuamente y se comparten entre diferentes organizaciones y proveedores de servicios para ayudar a proteger a los usuarios de posibles amenazas.

Las blacklists pueden ser creadas y mantenidas por diferentes entidades, como empresas de seguridad, proveedores de servicios de Internet (ISP), organizaciones gubernamentales y grupos de la comunidad de seguridad informática. Las direcciones IP, nombres de dominio o direcciones de

correo electrónico se agregan a las blacklists después de una evaluación de su reputación, historial de actividad y otros factores relevantes (Šuľan y Husák, 2022).

Es importante tener en cuenta que el uso de blacklists no es infalible y puede haber casos en los que se bloqueen recursos legítimos o se permita el acceso a recursos maliciosos que no están en la lista. Por lo tanto, el uso de blacklists debe complementarse con otras técnicas de seguridad informática, como firewalls, sistemas de detección de intrusiones y análisis de comportamiento de usuarios y sistemas (Imeri y Rysavy, 2023).

1.3.1 Aplicaciones para la Detección de Escaneos en Sistemas de Gestión de Contenidos Web

A partir de la clasificación de tecnologías antes enunciada puede decirse que existen diversos productos tecnológicos para ello. Dentro de los más reconocidos se encuentran:

Snort

Snort es un NIDS de código abierto y gratuito, diseñado para monitorear el tráfico de red y detectar posibles actividades maliciosas. Es considerado uno de los NIDS más populares y ampliamente utilizados en Cuba. Utiliza una combinación de reglas predefinidas y personalizadas para detectar patrones de tráfico de red sospechosos o maliciosos. Las reglas son escritas en un lenguaje de programación específico y describen las características del tráfico que se deben buscar, como patrones de paquetes, direcciones IP o puertos específicos.

Cuando Snort detecta un patrón sospechoso, genera una alerta que puede ser visualizada en una consola de administración o enviada a un sistema de gestión de eventos de seguridad (SIEM) para su análisis y respuesta. Además de su capacidad de detección de intrusiones, Snort también puede ser utilizado para la prevención de intrusiones (IPS), lo que significa que puede tomar medidas proactivas, como bloquear el tráfico sospechoso o malicioso.

Snort es altamente personalizable y puede ser utilizado en diferentes sistemas operativos y plataformas de hardware. Cuenta con una amplia comunidad de usuarios y desarrolladores que continúan mejorando y actualizando el software (Roesch, 2015).

Suricata

Suricata es un sistema de detección y prevención de intrusiones de red (en inglés: Intrusion Detection and Prevention System o IDPS) de código abierto y gratuito. Fue desarrollado por la organización Open Information Security Foundation (OISF) y es considerado uno de los sistemas más avanzados y eficientes en su categoría. Suricata utiliza una variedad de técnicas para analizar el tráfico de red en tiempo real y detectar patrones sospechosos. El sistema es capaz de inspeccionar el contenido de los

paquetes de red y detectar amenazas como malware, exploits, ataques de denegación de servicio (DoS) y actividades de botnets (Roesch y Markoff 2010).

Suricata, al igual que Snort es muy utilizado en Cuba. Además de su capacidad de detección de intrusiones, Suricata también ofrece funciones de prevención de intrusiones (IPS. Utiliza un lenguaje de reglas altamente expresivo, similar al utilizado por Snort, para definir patrones de tráfico de red sospechosos o maliciosos. Las reglas pueden ser personalizadas y ajustadas para adaptarse a las necesidades específicas de cada entorno. Es altamente escalable y puede ser utilizado en diferentes sistemas operativos y plataformas de hardware. También cuenta con una amplia comunidad de usuarios y desarrolladores que continúan mejorando y actualizando el software.

OSSEC

OSSEC (Open Source Security) es un sistema de detección de intrusiones de host (en inglés: Host Intrusion Detection System o HIDS) de código abierto y gratuito. Fue desarrollado por Trend Micro y es considerado uno de los HIDS más populares y ampliamente utilizados en la industria de la seguridad informática. Está diseñado para monitorear y analizar la actividad en sistemas individuales, incluyendo archivos, registros de sistema, contraseñas y otros aspectos relevantes. El sistema utiliza una combinación de técnicas de detección, como la monitorización de archivos, la verificación de integridad del sistema operativo y la detección de procesos maliciosos activos, para detectar cualquier actividad sospechosa (OSSEC, 2022).

Cuando OSSEC detecta una actividad sospechosa, genera una alerta que puede ser visualizada en una consola de administración o enviada a un sistema de gestión de eventos de seguridad (SIEM) para su análisis y respuesta. Es altamente personalizable y puede ser utilizado en diferentes sistemas operativos y plataformas de hardware. También cuenta con una amplia comunidad de usuarios y desarrolladores que lo mantienen y actualizan constantemente.

Además de su capacidad de detección de intrusiones, OSSEC también ofrece características de prevención de intrusiones (IPS) y de respuesta automática (Active Response), lo que significa que puede tomar medidas proactivas, como bloquear el tráfico sospechoso o malicioso, y responder automáticamente a posibles amenazas.

Wazuh

Wazuh es un HIDS de código abierto y gratuito, basado en OSSEC. Es desarrollado por la compañía Wazuh Inc. e incluye detección de intrusiones, prevención de intrusiones, monitoreo de logs, análisis de vulnerabilidades y cumplimiento normativo. Wazuh utiliza una arquitectura cliente-servidor, en la que los agentes Wazuh se instalan en los sistemas que se desean monitorear y envían la información

recopilada al servidor central Wazuh. El servidor central se encarga de analizar y correlacionar la información recibida de los agentes y generar alertas en caso de detectar alguna actividad sospechosa o maliciosa.

Wazuh también ofrece una interfaz web para la gestión y visualización de alertas, y es altamente personalizable y escalable, lo que lo hace adecuado para organizaciones de diferentes tamaños y necesidades (Wazuh Inc, 2022).

AbuseIPDB

AbuseIPDB es un servicio en línea gratuito que permite a los usuarios informar sobre direcciones IP que se han utilizado para llevar a cabo actividades maliciosas en línea, como spam, ataques de denegación de servicio (DoS), intentos de phishing, entre otros. El servicio se enfoca en la identificación y denuncia de actividades maliciosas en línea, y tiene como objetivo ayudar a mantener una red más segura para todos los usuarios.

Para utilizar AbuseIPDB, los usuarios pueden ingresar la dirección IP sospechosa en el sitio web de AbuseIPDB y enviar un informe detallado sobre la actividad sospechosa. El servicio luego procesa el informe y lo comparte con proveedores de servicios de Internet (ISP), organizaciones de seguridad informática y otros usuarios interesados para tomar medidas preventivas y de respuesta.

AbuseIPDB también proporciona una API para que los sistemas de seguridad informática puedan integrar la información de su base de datos en sus propios sistemas y tomar medidas preventivas y de respuesta más rápidamente. Es una herramienta útil para combatir el abuso de direcciones IP y la actividad maliciosa en línea. Al informar sobre posibles abusos de direcciones IP, los usuarios pueden ayudar a prevenir futuros ataques y mejorar la seguridad en línea para todos los usuarios (AbuseIPDB. s.f.).

1.3.2 Limitaciones de las soluciones informáticas para Detección de Escaneos en Sistemas de Gestión de Contenidos Web

Como ha sido analizado en las secciones anteriores, las soluciones informáticas analizadas proveen diferentes ventanas para la detección de diferentes tipos de ataques en sistemas informáticos, incluyendo aquellos realizados contra aplicaciones web. No obstante, deben señalarse algunas desventajas y limitaciones que estas poseen y que hacen necesario trabajar para su solución, especialmente en el contexto cubano:

1) Una parte importante de los protocolos de red están bloqueados para el acceso desde el exterior de la entidad con el objetivo de limitar la superficie de ataque, por lo que es relativamente simple para los sistemas de seguridad, la detección de ataques sobre los

mismos, por ejemplo un intento de conexión por SSH o Telnet, sin embargo, el protocolo HTTP, el cual es utilizado por las aplicaciones web, trabaja a nivel de la capa 7 (aplicación) del modelo OSI, lo que significa que es un protocolo cuya dinámica y funcionamiento va a depender de los procesos de negocio de la entidad lo que complejiza la elaboración de reglas estándares para definir en qué momento se está produciendo ciertos ataques.

2) Aunque los productos analizados son de código abierto, las bases de datos de firma de ataques o blacklist tienen una limitación de uso diaria o son meramente de pagos. Esto significa que no bastante con aplicar un sistema, sino que además es necesario contratar un servicio de actualización de firmas de ataques de calidad que permita el bloqueo de direcciones atacantes, sobre todo cuando se producen incidentes en tiempo real, limitación que como país tenemos por el uso de recursos financieros que esto puede conllevar.
3) Pueden producirse ataques especialmente diseñados contra Cuba y de los cuales, las bases de datos internacionales no tengan referencia. Por lo que la contratación de un servicio de actualizaciones de firma de seguridad no garantiza que se tenga en cuenta este tipo de ataque. Este razonamiento fue el que llevó a la creación de una empresa como Segurmática en Cuba, cuestión que se justificó con la detección de malware especialmente diseñado para el país y que no aparece en las bases de datos internacionales.
4) La suscripción a los servicios de blacklist incluye el chequeo de las posibles direcciones IP atacantes, por lo que se está suministrando información a un proveedor internacional que bajo ciertas circunstancias puede ser información sensible para el país. Por ejemplo, supongamos que el mismo actor de amenaza estado-nación controla un servicio de blacklist contratado por Cuba, si es el caso, el propio proceso de chequeo de las direcciones IP atacantes puede suministrarle información a este agente sobre la detección o no de las direcciones IP atacantes que está empleando, lo que le permitirá tomar decisiones para cambiar de direcciones IP y sostener el ataque en el tiempo.
5) Para entrenar los modelos heurísticos de inteligencia artificial muy utilizados en estas herramientas de seguridad, en necesario contar con una base de datos de casos adecuadamente gestionado de manera tal que puedan aprender del comportamiento de los ataques y actuar en correspondencia. Sin embargo, esta información es cuidadosamente ocultada a los usuarios por la importancia que se requiere y limita la capacidad de los desarrolladores para entrenar nuevos modelos que garanticen una soberanía tecnológica en este sentido.

Una vez definidas estas limitantes se puede concluir que es necesario la implementación de una herramienta que permita al país contar con una base de direcciones IP sospechosas que pueda ser consultada por los especialistas de ciberseguridad para consultar IP sospechosas.

1.4 Tecnologías y herramientas utilizadas para el desarrollar un sistema informático para la detección de escaneos

Para la selección de las herramientas a utilizar parala realización de la propuesta de solución se tuvo en cuenta que la presente investigación forma parte de un proyecto sectorial de ciberseguridad perteneciente al grupo de investigación de ciberseguridad de la UCI. Este proyecto tiene definidos un conjunto de herramienta para la concepción de los productos que deben desarrollarse como parte del mismo. Las herramientas definidas son:

HTML5

HTML5 es la quinta versión del lenguaje de marcado HTML (Hypertext Markup Language), utilizado para la estructuración y presentación del contenido en los sitios web. HTML5 ofrece nuevas funcionalidades y mejoras con respecto a versiones anteriores de HTML, incluyendo la incorporación de elementos semánticos que permiten una mejor descripción del contenido, la posibilidad de incorporar audio y video sin necesidad de plugins externos, y una mayor capacidad para trabajar con aplicaciones web offline.

Además, HTML5 incluye nuevas características para la accesibilidad, como la especificación de atributos para los formularios y las etiquetas, y la posibilidad de definir contenido alternativo para los elementos multimedia. También ofrece mejoras en cuanto a la compatibilidad con dispositivos móviles, permitiendo que los sitios web se adapten mejor a diferentes tamaños de pantalla y dispositivos (Duckett, 2011).

CSS3

CSS3 es la tercera versión del lenguaje de hojas de estilo en cascada (Cascading Style Sheets), utilizado para el diseño de la presentación de los sitios web. CSS3 ofrece nuevas funcionalidades y mejoras con respecto a versiones anteriores de CSS, incluyendo la incorporación de nuevas propiedades de diseño, selectores avanzados y animaciones. Entre las nuevas propiedades de diseño se encuentran la posibilidad de trabajar con bordes redondeados, sombras, gradientes, transformaciones y transiciones. Estas propiedades permiten una mayor flexibilidad en el diseño y una mayor capacidad para crear efectos visuales en los sitios web (Meyer y Lea 2020).

CSS3 incluye selectores avanzados que permiten seleccionar elementos específicos de una página web basándose en su posición, estado o relación con otros elementos. También ofrece nuevas

funcionalidades para trabajar con fuentes, como la posibilidad de incorporar fuentes personalizadas en los sitios web.

JavaScript

JavaScript es un lenguaje de programación interpretado que se utiliza principalmente en el desarrollo de aplicaciones web. Fue creado por Netscape en 1995 y desde entonces ha evolucionado para convertirse en uno de los lenguajes de programación orientado a objeto y basado el prototipos más populares y utilizados del mundo. Se utiliza para crear interactividad en la página web, como la validación de formularios, la creación de animaciones, la manipulación del DOM (Document Object Model), la interacción con servidores, entre otros (Flanagan, 2020).

JavaScript es compatible con todos los navegadores web modernos y se ejecuta directamente en el navegador del cliente, por lo que no se necesita ningún software adicional para utilizarlo. Además, se puede utilizar en el servidor a través de plataformas como Node.js.

Python

Python es un lenguaje de programación de alto nivel, interpretado y multiparadigma que se utiliza en una amplia variedad de aplicaciones, desde el desarrollo de aplicaciones web hasta la ciencia de datos, inteligencia artificial, automatización de tareas y otros.Fue creado a finales de los años 80 por Guido van Rossum y se caracteriza por su legibilidad y sintaxis clara, lo que lo hace fácil de aprender y utilizar. Python es un lenguaje de programación interpretado, lo que significa que se ejecuta en tiempo real a medida que se escribe el código, lo que lo hace ideal para la programación interactiva y el prototipado rápido.

Python es un lenguaje de programación multiparadigma, lo que significa que admite varios estilos de programación, incluyendo programación orientada a objetos, programación imperativa y programación funcional. Además, cuenta con una amplia biblioteca estándar que incluye módulos para tareas comunes como el manejo de archivos, la conexión a bases de datos, la manipulación de datos entre otros (Van Rossum y Drake 2021).

Python es también un lenguaje de programación multiplataforma, lo que significa que se puede ejecutar en diferentes sistemas operativos, como Windows, macOS y Linux, entre otros. Es utilizado por muchas organizaciones, incluyendo Google, NASA, Dropbox, Instagram, entre otros.

Visual Studio Code

Visual Studio Code es un editor de código fuente gratuito y de código abierto desarrollado por Microsoft. Es compatible con múltiples lenguajes de programación y se puede usar en diferentes sistemas operativos, como Windows, macOS y Linux.

Visual Studio Code tiene una amplia gama de características, como resaltado de sintaxis, autocompletado de código, depuración de código, control de versiones integrado, integración con herramientas de construcción y pruebas, y una gran cantidad de extensiones que pueden personalizar el editor para satisfacer las necesidades de los desarrolladores.

Además, Visual Studio Code tiene una interfaz de usuario intuitiva y fácil de usar, lo que lo hace accesible para desarrolladores de diferentes niveles de experiencia. Por todas estas razones, Visual Studio Code se ha convertido en uno de los editores de código más populares entre los desarrolladores (Microsoft Corporation, 2022).

PosgreSQL

PostgreSQL es un sistema de gestión de bases de datos relacional de código abierto y gratuito. Es uno de los sistemas de bases de datos más avanzados y potentes disponibles en la actualidad, y se utiliza en muchas aplicaciones. Es altamente escalable, lo que significa que puede manejar grandes volúmenes de datos y una gran cantidad de usuarios simultáneamente. Ofrece un amplio conjunto de características, incluyendo soporte para múltiples plataformas, transacciones ACID (Atomicidad, Consistencia, Aislamiento y Durabilidad), integridad referencial, vistas, desencadenadores, almacenamiento de procedimientos almacenados y funciones, y soporte para múltiples lenguajes de programación.

PostgreSQL tiene una arquitectura modular y extensible que permite a los usuarios personalizar y ampliar la funcionalidad del sistema de bases de datos según sus necesidades específicas. También cuenta con una comunidad activa de desarrolladores y usuarios que trabajan en su mejora y evolución continua (The PostgreSQL Global Development Group, 2021).

Visual Paradigm

Visual Paradigm es una suite de herramientas de modelado y diseño de software utilizada por desarrolladores, arquitectos de software y otros profesionales de TI para crear diagramas y modelos de software. Permite realizar diagramas UML, diagramas de flujo de datos, diagramas de clases, diagramas de secuencia, diagramas de actividad, diagramas de componentes y muchos más. También ofrece herramientas de colaboración y gestión de proyectos, que permiten a los usuarios trabajar juntos y gestionar proyectos de software de manera efectiva (Visual Paradigm International, 2021).

Es compatible con diferentes lenguajes de programación y entornos de desarrollo, lo que lo convierte en una opción muy utilizada para desarrolladores y arquitectos de software que trabajan en diferentes plataformas y tecnologías.

Django como Framework de desarrollo

Django es un framework de desarrollo web de alto nivel y de código abierto, escrito en Python. Se utiliza para desarrollar aplicaciones web complejas y escalables. Brinda características y funcionalidades que incluyen un ORM (Mapeo objeto-relacional) para interactuar con la base de datos, un sistema de autenticación y autorización de usuarios, un sistema de plantillas para la creación de interfaces de usuario, un sistema de enrutamiento de URLs, un sistema de cache, soporte para diferentes tipos de bases de datos, y muchas más. Es altamente modular y extensible, por lo que los desarrolladores pueden personalizar y extender el framework según sus necesidades específicas (The Django Software Foundation,2020).

Bootstrap

Bootstrap es un framework de diseño web de código abierto y gratuito, desarrollado por Twitter. Se utiliza para crear sitios web y aplicaciones web responsivos y móviles, que se adaptan automáticamente a diferentes tamaños de pantalla y dispositivos. Incluyen un sistema de grid (cuadrícula) para la creación de diseños flexibles, un conjunto de componentes predefinidos (como botones, formularios, menús, etc.), un sistema de tipografía, un sistema de iconos, y muchas más. Es personalizable, extensible y compatible con los navegadores y dispositivos modernos, por lo que se utiliza para trabajar en aplicaciones en diferentes plataformas y tecnologías.

Librerías de JavaScript

JQuery

jQuery es una biblioteca de JavaScript de código abierto y gratuita, que se utiliza para simplificar la manipulación de elementos HTML y la interacción con el DOM (Modelo de objeto de documento) en sitios web y aplicaciones web. Permite realizar tareas comunes de programación en el lado del cliente, como la manipulación de elementos HTML, el manejo de eventos, la animación, la navegación y la comunicación con el servidor. Es compatible con diferentes navegadores, dispositivos, plataformas y tecnologías. Los desarrolladores pueden adaptar la biblioteca según sus necesidades específicas.

Highcharts

Highcharts es una biblioteca de gráficos interactivos de JavaScript de alta calidad, que se utiliza para crear gráficos y visualizaciones de datos en sitios web y aplicaciones web. Brinda una amplia variedad de tipos de gráficos, que incluyen gráficos de líneas, gráficos de barras, gráficos circulares, gráficos de área, gráficos de dispersión, capacidad de generar gráficos en tiempo real, animaciones y efectos visuales, y la integración con otras bibliotecas y frameworks de JavaScript.

Metodología de desarrollo de software

Algunos autores definen una metodología como una colección de procedimientos, técnicas, herramientas y documentos auxiliares que ayudan a los desarrolladores de software en sus esfuerzos por implementar nuevos sistemas de información (Maida y Pacienzia, 2015). Existen dos paradigmas cuando se habla de metodologías de software, las tradicionales o robustas y las ágiles. La tabla 1 muestra las principales características de cada una de ellas.

Tabla 1 Diferencias entre Metodologías Tradicionales y Agiles

Metodologías Tradicionales	Metodologías Agiles
Basadas en normas provenientes de estándares seguidos por el entorno de desarrollo. Cierta resistencia a los cambios.	Basadas en heurísticas provenientes de prácticas de producción de código. Especialmente preparados para cambios durante el proyecto.
Impuestas externamente. Proceso mucho más controlado, con numerosas políticas/normas.	Impuestas internamente (por el equipo). Proceso menos controlado, con pocos principios.
El cliente interactúa con el equipo de desarrollo mediante reuniones y presenta más artefactos.	El cliente es parte del equipo de desarrollo, presenta pocos artefactos.
Más roles, grupos grandes y posiblemente distribuidos.	Pocos roles, grupos pequeños (menos de 10 integrantes) y trabajando en el mismo sitio.
La arquitectura del software es esencial y se expresa mediante modelos, existe un contrato prefijado	Menos énfasis en la arquitectura del software, no existe contrato tradicional o al menos es bastante flexible.

El método de Boehm y Turner plantea 5 criterios fundamentales mediante los que se valora el proyecto; estos son: **tamaño del equipo**, **criticidad del producto**, **dinamismo de los cambios, cultura del equipo** y **personal con que se cuenta**. Cada uno de esos criterios tiene elementos que lo discriminan y por tanto se tienen en cuenta a la hora de seleccionar uno u otro enfoque. Para la selección del valor que se ubicará en cada eje (uno para cada criterio) de la estrella se debe tener en cuenta el comportamiento de estos criterios en el proyecto como se observa en la *Figura 3* se describe cada uno (Boehm y Turner, 2003)

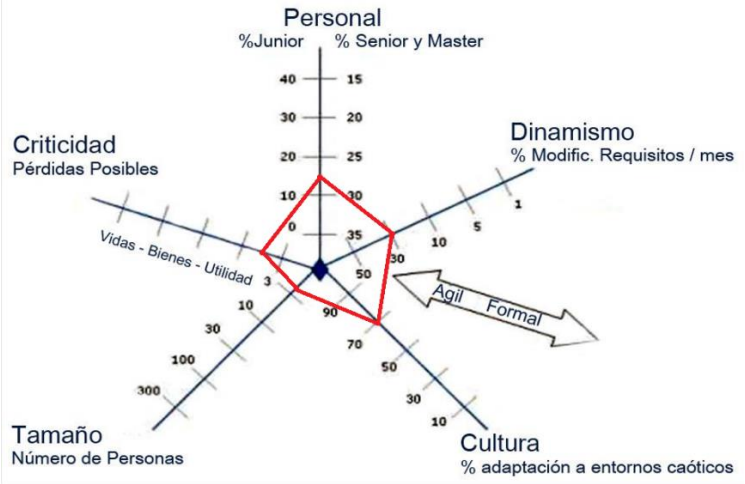


Figura 3. Estrella de Boehm y Turner

Tamaño: Para el desarrollo de la presente solución se cuenta con un equipo de trabajo pequeño, compuesto por un desarrollador y el cliente. El desarrollador cuenta con disimiles vías de comunicación, lo que facilita y promueve el trabajo con el cliente.

Criticidad: Se estima que, en caso de errores no detectados en la solución, los daños sean mínimos y no pasen más allá de afectar las utilidades.

Dinamismo: Teniendo en cuenta la facilidad que existe en la comunicación entre desarrollador y el cliente, los cambios que puedan surgir en el transcurso del desarrollo de la solución se resuelven en el menor tiempo posible.

Personal: El miembro del equipo cuentan con un nivel medio de experiencia, pues ha enfrentado en otras ocasiones el desarrollo de una solución completa, además de tener cierto dominio de las tecnologías utilizadas.

***Cultura*:** El equipo de desarrollo cuenta con la habilidad y capacidad de adaptación a situaciones críticas, siendo capaces de solucionarlas sin llegar a afectar el desarrollo de la solución.

Luego del análisis de la estrella de Boehm y Turner, se llega a la conclusión que la metodología a utilizar sea con enfoque ágil. Según (Yánez Triana, 2022) las metodologías ágiles más usadas hoy en día son Scrum y Extreme Programming (XP). A continuación, se muestra una tabla comparativa desarrollada por el equipo de trabajo que facilita la selección de la metodología ágil que más se ajusta a la investigación según las condiciones actuales de este proceso.

Tabla 2 Comparación Scrum y XP

Parámetro de calidad	Extreme Programming (XP)	Scrum

El cliente forma parte del equipo de desarrollo	Si	No
Aceptar cambios en cualquier momento de alguna iteración	Si	No
Programación en pareja	Si	No
Tamaño del proyecto	Bajo-Medio	Medio-Alto
Tamaño del equipo	< 10	<10 y múltiples equipos
Auto organización	No	Si

Luego del análisis descrito en la Tabla 2, la metodología ágil que más se ajusta a la investigación es XP, pues se adecúa al desarrollo del siguiente trabajo y a los contextos en que se realiza el mismo. El cliente forma parte del equipo de desarrollo del proyecto, logrando una realimentación continua y corrección de errores. El proyecto a desarrollar es pequeño y cuenta con un solo equipo, donde todo el trabajo se realiza por una pareja de programadores. A la par que progresa el proyecto, el cliente puede agregar nuevas historias de usuario, modificadas, o eliminarlas. Permite al equipo la modificación de sus planes en correspondencia con los anteriores. El proyecto está ajustado en ser desarrollado en seis meses, además de probar los resultados que se vayan obteniendo en cada iteración.

Metodología XP

Dentro de las metodologías de desarrollo de software se encuentra la programación extrema o Extreme Programming (XP), según Kent Beck, ingeniero estadounidense que formuló este enfoque de la Ingeniería de Software y autor del primer libro sobre la materia, “Extreme Programming Explained: Embrace Change” (1999), “Es el más destacado de los procesos ágiles de desarrollo de software”. XP se diferencia de las metodologías tradicionales principalmente en que pone más énfasis en la adaptabilidad que en la previsibilidad. Se aplica de manera dinámica durante el ciclo de vida del software. Es capaz de adaptarse a los cambios de requisitos. XP aboga por un correcto funcionamiento del software más que por una documentación exhaustiva. La colaboración con el cliente es más importante que la negociación de contratos. La respuesta ante el cambio es más significativa que el seguimiento de un plan. Además, potencia las relaciones interpersonales como clave para el éxito en el desarrollo de software; promueve el trabajo en equipo, preocupándose por el aprendizaje de los desarrolladores; y propicia un buen clima de trabajo. XP se basa en realimentación continua entre el cliente y el equipo de desarrollo, comunicación fluida entre todos los participantes, simplicidad en las soluciones implementadas y coraje para enfrentar los cambios. Además, cumple con el ciclo que se muestra en la *Figura 4* (Stray et al., 2020).

Figura 4. Ciclo de la metodología XP

1.5 Conclusiones del capítulo

En el epígrafe se sistematización los fundamentos teórico-metodológicos asociados a las tecnologías y herramientas que se utilizaron para lograr el resultado contenido en el campo de acción y que fue reflejado en el objetivo general de la investigación; así como se explica el porqué de la selección de las tecnologías para el desarrollo del sistema.

CAPÍTULO II: DISEÑO DE LA SOLUCIÓN PROPUESTA AL PROBLEMA CIENTÍFICO

2.1 Introducción al Capítulo

Este capítulo contiene las características asociadas al dominio de la aplicación; la propuesta de solución del sistema a desarrollar, el rol definido para administrar y proveer la seguridad a la aplicación. Las funcionalidades se describen mediante las historias de usuario (HU). Se realiza el plan de iteraciones donde se muestran las HU a realizar en cada iteración según su prioridad en el negocio. Se lleva a cabo la realización del plan de entrega, donde se indican las HU que se implementarán para cada entrega de la aplicación propuesta, así como las fechas en las que se realizarán las mismas.

2.2 Propuesta de Solución

Después de evaluar las necesidades del sistema y elegir las herramientas apropiadas para su implementación, se procede a definir los módulos que se deben desarrollar para abordar la problemática planteada, figura 5:

Figura 5 Propuesta de Solución. Elaboración Propia

- **Módulo IP**: Tiene como objetivo gestionar los datos relativos a las direcciones IP sospechosas como: país de procedencia y la propia dirección IP.
- **Módulo Petición**: Tiene como propósito gestionar las características de las peticiones HTTP sospechosas. Incluye la fecha y hora en que se realizó la petición, dirección IP empleada, el método HTTP utilizado, el código de respuesta HTTP, el agente de usuario empleado, la referencia contenida, la URL y el incidente.
- **Módulo Incidente**: Tiene como objetivo registrar los incidentes en los que se han visto involucradas las peticiones y direcciones IP sospechosas. Esto incluye el nombre del incidente, una breve descripción del incidente, la fecha en que se produjo, la tecnología involucrada víctima del incidente, la clasificación del incidente y la entidad afectada.
- **Módulo Usuario**: Tiene como propósito gestionar los usuarios que interactuarán con el sistema, así como la creación de grupos y roles.
- **Módulo Portal**: Contiene diferentes reportes sobre las direcciones IP y las peticiones sospechosas contenidas en la base de datos y posibilita a los usuarios buscar direcciones IP en la base de datos.

Como la solución está enfocada fundamentalmente a la interacción automatizada con otros sistemas de seguridad, adicionalmente a la investigación se provee un API REST (Interfaz de Programación de Aplicaciones de Transferencia de Estado Representacional) para la interoperabilidad con estos sistemas.

2.3 Fase I. Planificación.

La etapa inicial del proyecto implica definir el alcance general. Durante esta fase, el cliente explica sus necesidades mediante la creación de HU y les asigna su nivel de prioridad. Después, los programadores calculan el tiempo de desarrollo basándose en esta información. Aunque estas estimaciones son preliminares, ya que se basan en datos generales y podrían variar en cada iteración. También se llega a acuerdos sobre el contenido de la primera entrega y se establece un cronograma en colaboración con el cliente. Es importante que la primera entrega se consiga en un plazo máximo de tres meses (ESCRIBANO, 2002; JOSKOWICZ, 2008)

2.3.1 Historias de Usuarios.

Las HU son las técnicas utilizadas por la metodología XP para especificar los requisitos del software, son equivalentes a los casos de uso en el proceso unificado y constituyen la base para las pruebas

funcionales. Se trata de tarjetas de papel en las cuales el cliente describe brevemente las características que el sistema debe poseer.

En las HU se considera:

La prioridad en el negocio:

- Muy Alta: Cuando son consideradas por los clientes esenciales para el funcionamiento del negocio.
- Alta: Cuando son consideradas necesarias por los clientes, para el funcionamiento del negocio, e intervienen directamente en el desarrollo del negocio.
- Media: Cuando el cliente cree que son necesarias, pero estas no intervienen en gran medida en el desarrollo del negocio.
- Baja: Cuando constituyen procesos que se deben tener en cuenta, pero su ausencia no perjudica el flujo principal del negocio.

El riesgo en desarrollo:

- Alto: Cuando en la implementación de las HU pueden surgir errores que lleven a la inoperatividad del código.
- Medio: Cuando en la implementación de las HU pueden existir errores que retrasen la entrega del producto.
- Bajo: Cuando pueden aparecer errores que serán tratados con relativa facilidad sin que traigan perjuicios para el desarrollo del proyecto.

Teniendo en cuenta el uso del framework de desarrollo Django se decide agrupar las funcionalidades y describirlas como CRUD completos en el caso de las que proceden, pues la programación se realiza de manera sencilla y prácticamente con un esfuerzo mínimo teniendo en cuenta las funcionalidades que ofrece dicho framework, además se establece que una semana contará con 4 días laborables, teniendo en cuenta que se está trabajando a tiempo completo en una empresa y no se puede disponer de los 7 días para desarrollar la investigación, por lo que una semana equivalen a 4 días laborables.

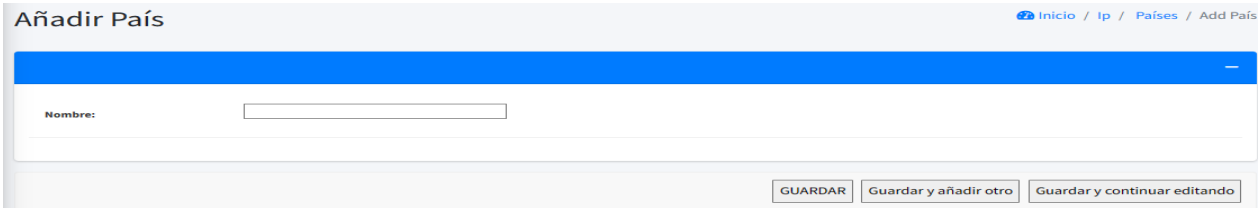
Tabla 3 Historia de Usuario #1

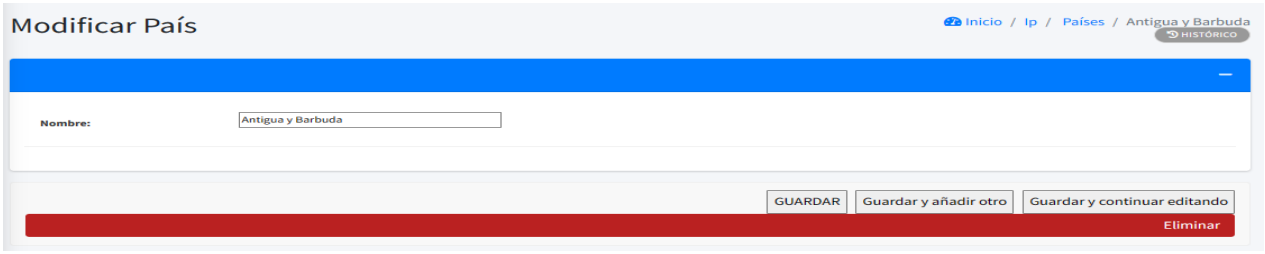
Historia de Usuario	
Número: HU_1	**Requisito:** Gestionar País
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 0.3	**Iteración Asignada:** 1
Programador responsable: Yadira Sánchez Cruz	

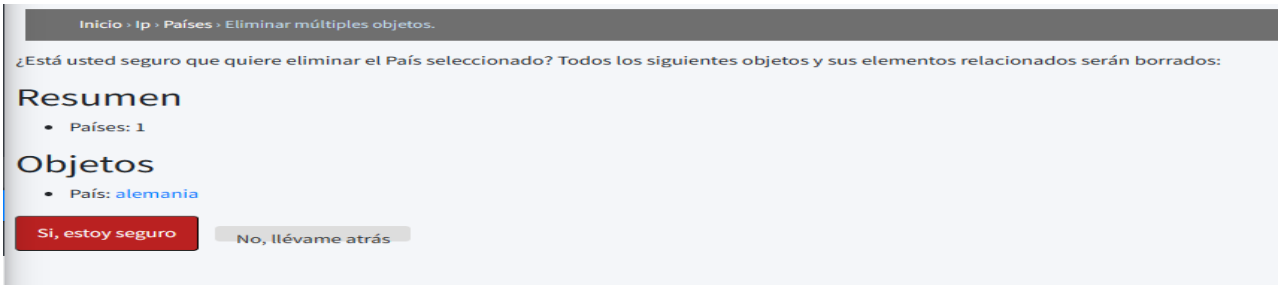
Descripción: El administrador requiere gestionar los datos de los países de los que se han realizado peticiones sospechosas, para lo cual se muestra una lista de los mismos con su identificador y su nombre y se presentan las opciones de buscar, adicionar, modificar y eliminar.

- **buscar país**: para ello, se teclea el nombre del país que se quiere buscar y se muestra el identificador y el nombre del país seleccionado, en caso de no encontrarse el país se muestra que: “El país no fue encontrado”
- **adicionar país**: para ello se introduce el nombre del país de donde procede la petición sospechosa, al adicionarse se muestra el mensaje: El País “nombre del país” fue agregado correctamente, en caso de que exista el país se especifica que ya existe un país con ese nombre.
- **modificar país**: para ello se busca el nombre del país que se quiere modificar y se cliquea sobre el mismo, al modificar se muestra el mensaje: El País “nombre del país” se cambió correctamente.
- **eliminar país**: para ello se selecciona el país que se quiere eliminar, antes de eliminarlo se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar el País seleccionado? Todos los siguientes objetos y sus elementos relacionados serán eliminados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 País satisfactoriamente.

Prototipo elemental de interfaz gráfica de usuario:







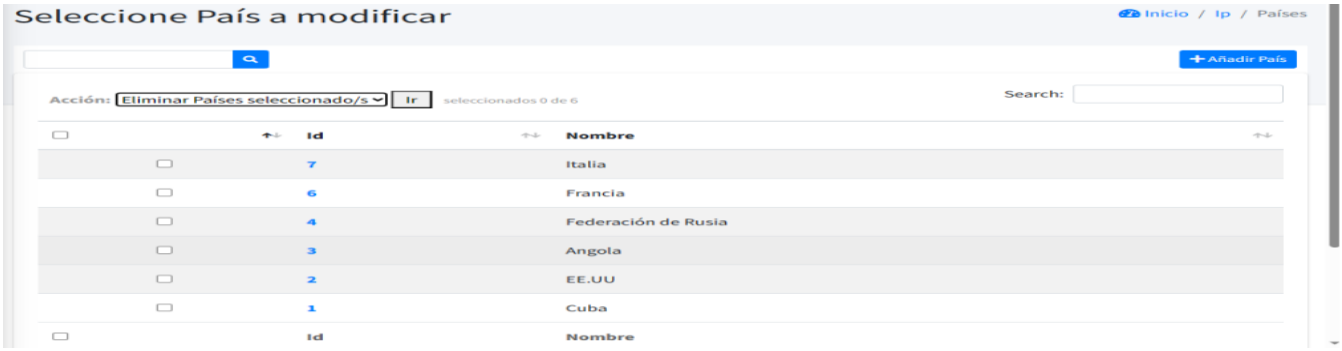


Tabla 4 Historia de Usuario # 11

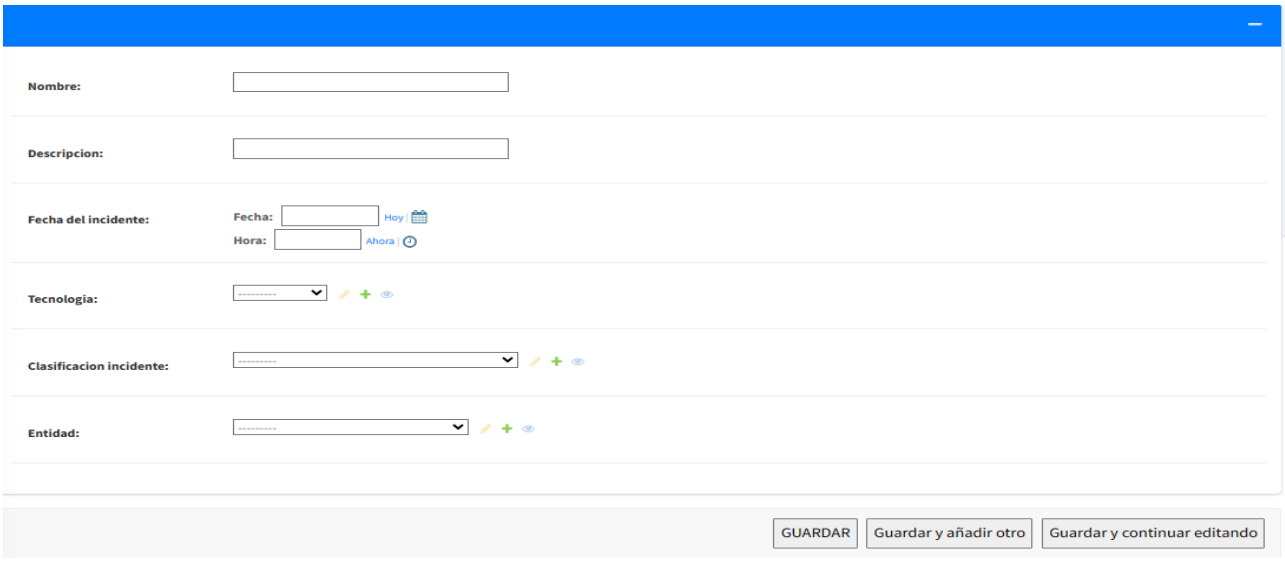
Historia de Usuario	
Número: HU_11	**Requisito:** Gestionar Incidente
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Alta
Puntos estimados: 1.2	**Iteración Asignada:** 2
Programador responsable: Yadira Sánchez Cruz	

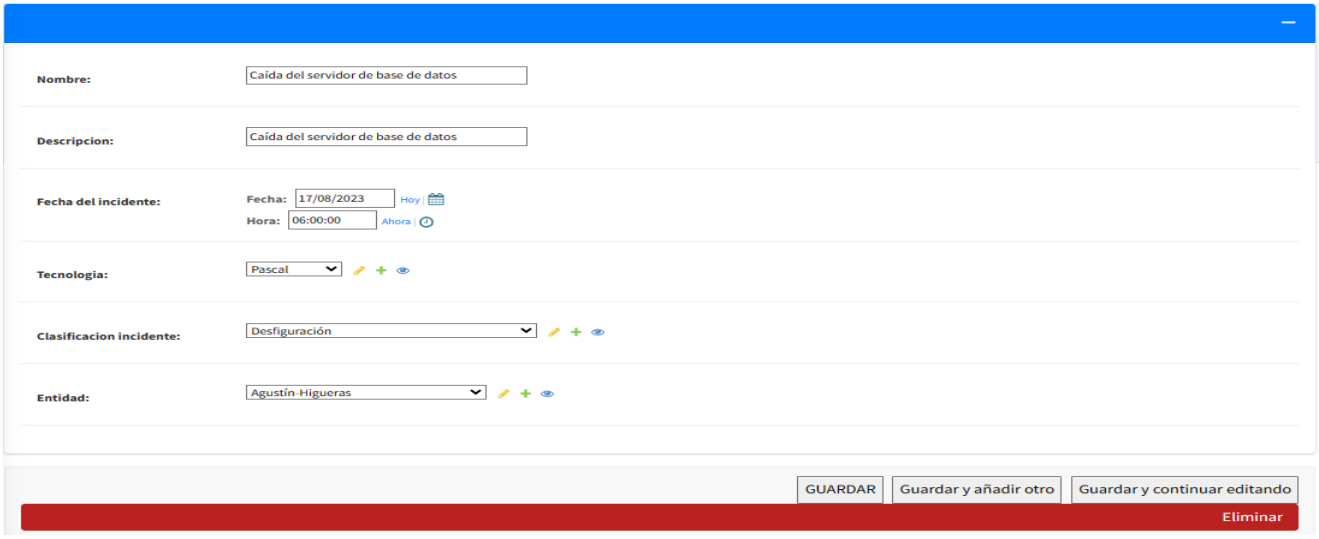
Descripción: El administrador requiere gestionar los datos de los incidentes ocurridos por las peticiones sospechosas, para lo cual se muestra una lista de los mismos con su identificador, nombre del incidente, descripción del incidente, la fecha del incidente, tecnología afectada, la clasificación del incidente y la entidad que afectó, y se presentan las opciones de buscar, adicionar, modificar y eliminar.

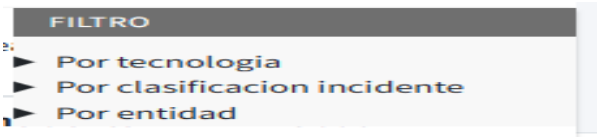
- **buscar incidente**: para ello, se teclea el nombre del incidente que se quiere buscar y como resultado se muestra el identificador, el nombre, la descripción, la fecha del incidente, la tecnología, la clasificación del incidente y la entidad, en caso de no encontrarse él incidente se muestra que: “El incidente no fue encontrado”
- **adicionar incidente**: para ello se introducen los datos del incidente (nombre, descripción, fecha, tecnología clasificación y entidad), al adicionarse se muestra un mensaje: El Incidente “nombre del incidente” fue agregado correctamente, en caso de que exista el incidente se muestra que ya existe el incidente con los datos proporcionados.
- **modificar incidente**: para ello se busca el incidente que se quiere modificar y se cliquea sobre el mismo, al modificar se muestra un mensaje: El Incidente “nombre del incidente” se cambió correctamente.
- **eliminar incidente**: para ello se selecciona el incidente que se quiere eliminar, antes de eliminarlo se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar el incidente seleccionado? Todos los siguientes objetos y sus elementos relacionados serán borrados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 Incidente satisfactoriamente

- **filtrar**: se tiene la posibilidad además de poder filtrar los incidentes por tecnología, clasificación del incidente y por entidad.

Prototipo elemental de interfaz gráfica de usuario:







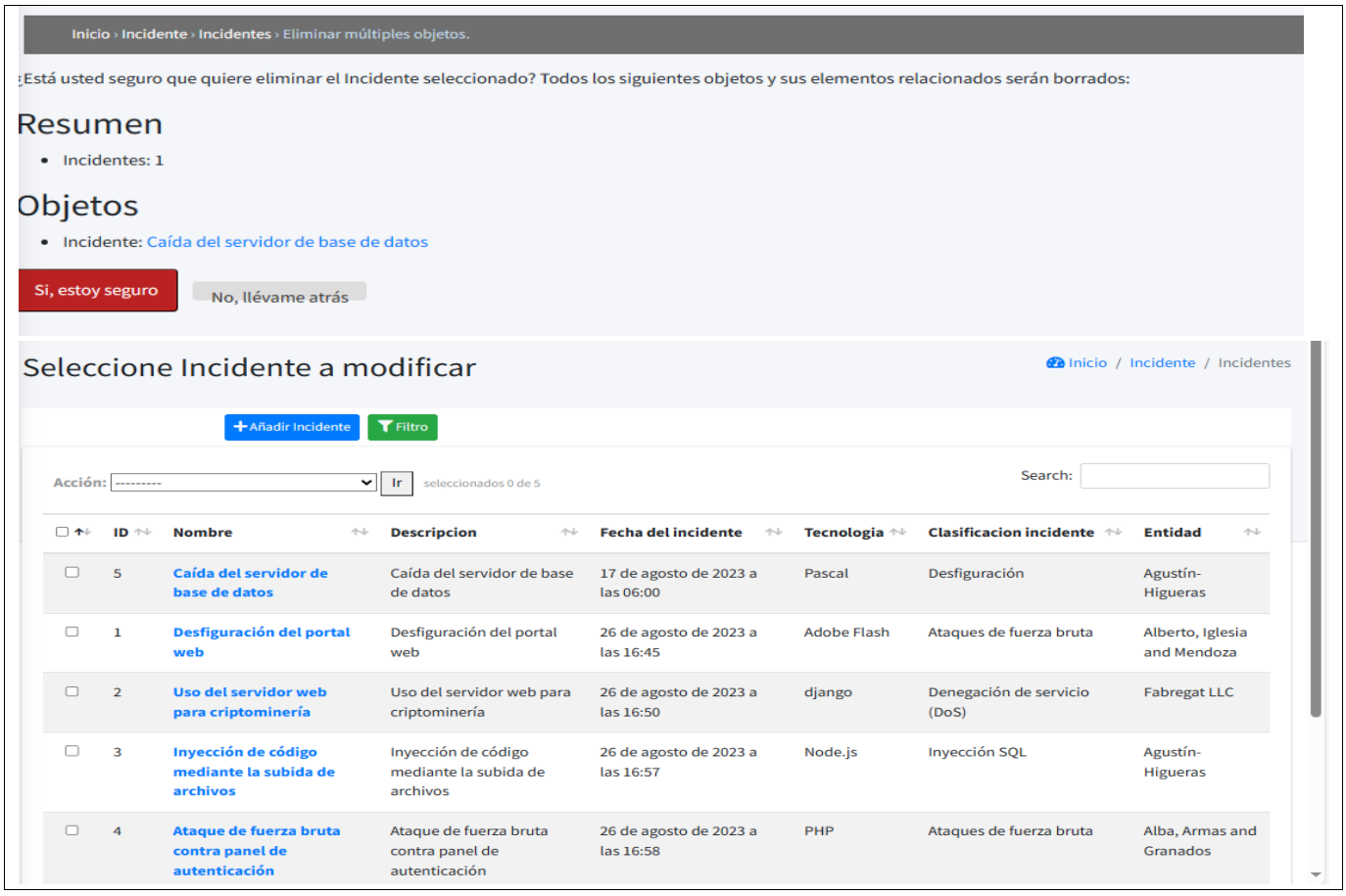


Tabla 5 Historia de Usuario #12

Historia de Usuario	
Número: HU_12	**Requisito:** Gestionar Peticiones
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Alta
Puntos estimados: 1.2	**Iteración Asignada:** 2
Programador responsable: Yadira Sánchez Cruz	

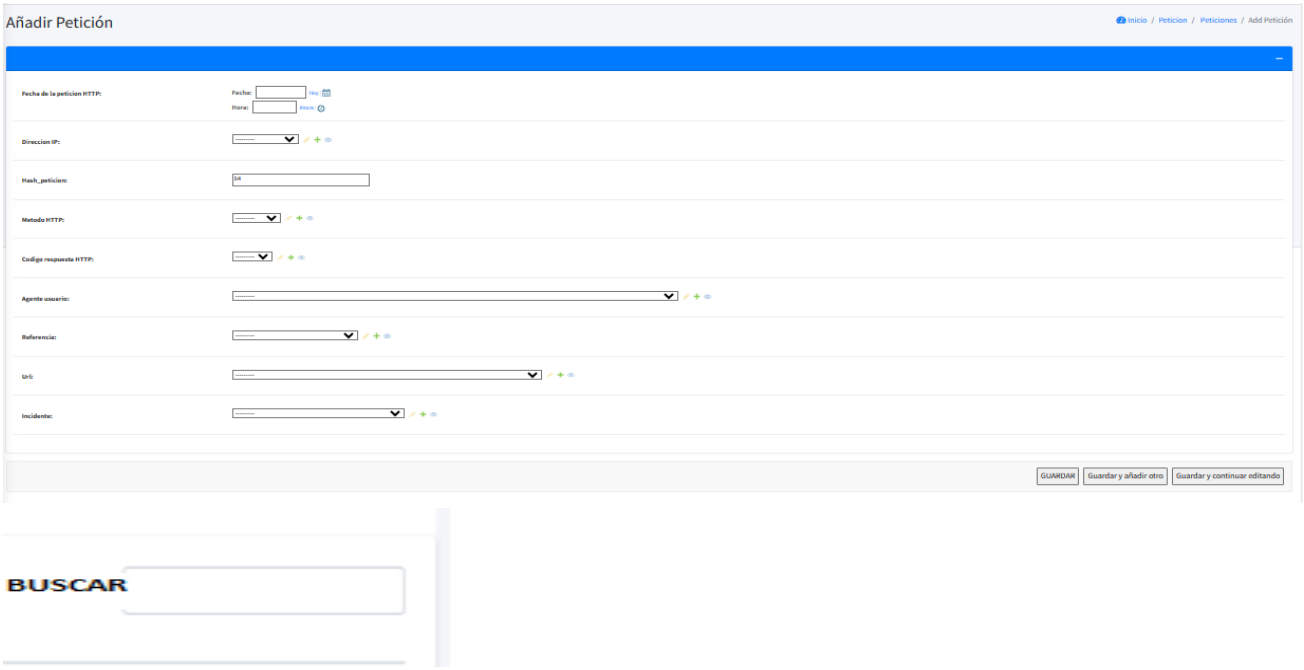
Descripción: El administrador requiere gestionar los datos de las peticiones sospechosas, para lo cual se muestra una lista de los mismos con su identificador, fecha de la petición HTTP, URL utilizada, dirección IP utilizada, método HTTP utilizado, código de respuesta HTTP, agente de usuario, referencia e incidente, y se presentan las opciones de buscar, adicionar, modificar y eliminar.

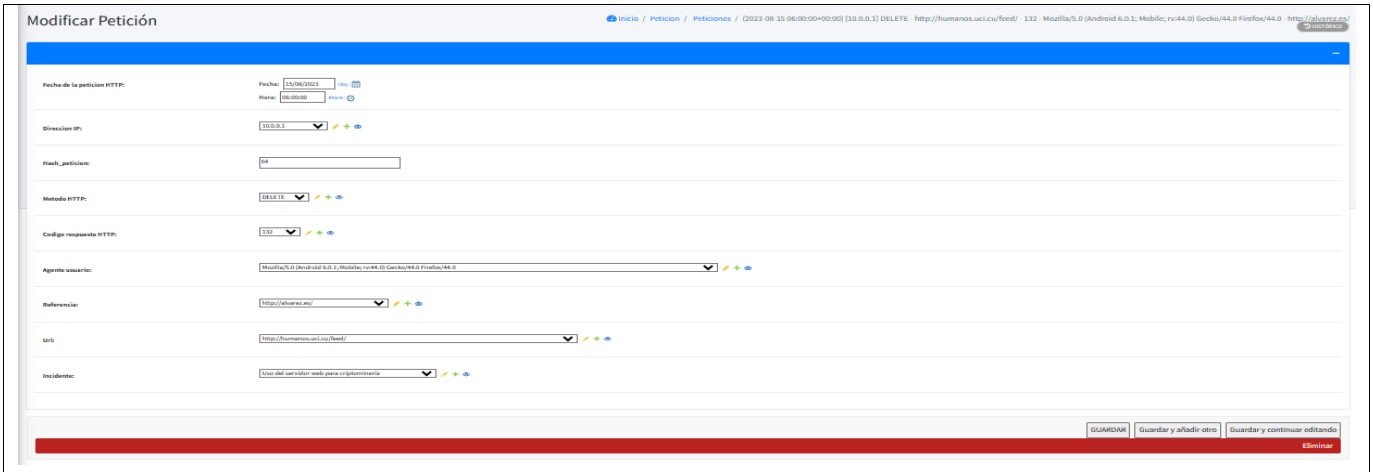
- **buscar petición**: para ello, se teclea la petición que se quiere buscar y como resultado se muestra el identificador, la fecha de la petición HTTP, URL, dirección IP, método HTTP, código de respuesta HTTP, agente de usuario, referencia y el incidente, en caso de no encontrarse la petición se muestra que: “La petición no fue encontrada”
- **adicionar petición**: para ello se introducen los datos de la petición (fecha de la petición HTTP, URL, agente de usuario, dirección IP, método HTTP, código de respuesta HTTP, referencia e

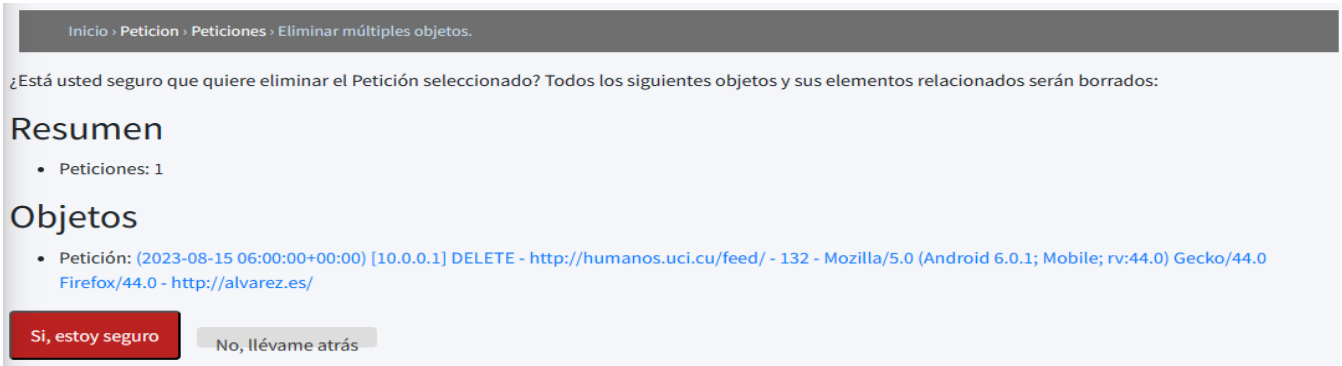
incidente), al adicionarse se muestra un mensaje: La petición “petición” fue agregada correctamente, en caso de que exista la petición se muestra que ya existe la petición con los datos proporcionados.

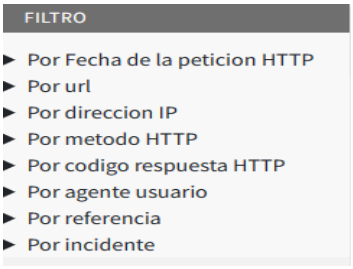
- **modificar petición**: para ello se busca la petición que se quiere modificar y se cliquea sobre la misma, al modificar se muestra un mensaje: La petición “petición” se cambió correctamente.
- **eliminar petición**: para ello se selecciona la petición que se quiere eliminar, antes de eliminarla se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar la petición seleccionada? Todos los siguientes objetos y sus elementos relacionados serán borrados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 Petición satisfactoriamente
- **filtrar**: se tiene la posibilidad además de poder filtrar las peticiones por fecha de la petición HTTP, URL, dirección IP, método HTTP, código de respuesta HTTP, agente de usuario, referencia y el incidente
-

Prototipo elemental de interfaz gráfica de usuario:




Modificar Petición
Inicio / Peticion / Peticiones / (2023-08-15 06:00:00+00:00) [10.0.0.1] DELETE - http://humanos.uci.cu/feed/ - 132 - Mozilla/5.0 (Android 6.0.1; Mobile; rv:44.0) Gecko/44.0 Firefox/44.0 - http://alvarez.es/
Fecha de la peticion HTTP:
Direccion IP:
Hash_peticion:
Metodo HTTP:
Codigo respuesta HTTP:
Agente usuario:
Referencia:
Url:
Incidente:
GUARDAR
Guardar y añadir otro
Guardar y continuar editando
Eliminar


Inicio › Peticion › Peticiones › Eliminar múltiples objetos.
¿Está usted seguro que quiere eliminar el Petición seleccionado? Todos los siguientes objetos y sus elementos relacionados serán borrados:
Resumen
Peticiones: 1
Objetos
Petición: (2023-08-15 06:00:00+00:00) [10.0.0.1] DELETE - http://humanos.uci.cu/feed/ - 132 - Mozilla/5.0 (Android 6.0.1; Mobile; rv:44.0) Gecko/44.0 Firefox/44.0 - http://alvarez.es/
Si, estoy seguro
No, llévame atrás


FILTRO
Por Fecha de la peticion HTTP
Por url
Por direccion IP
Por metodo HTTP
Por codigo respuesta HTTP
Por agente usuario
Por referencia
Por incidente

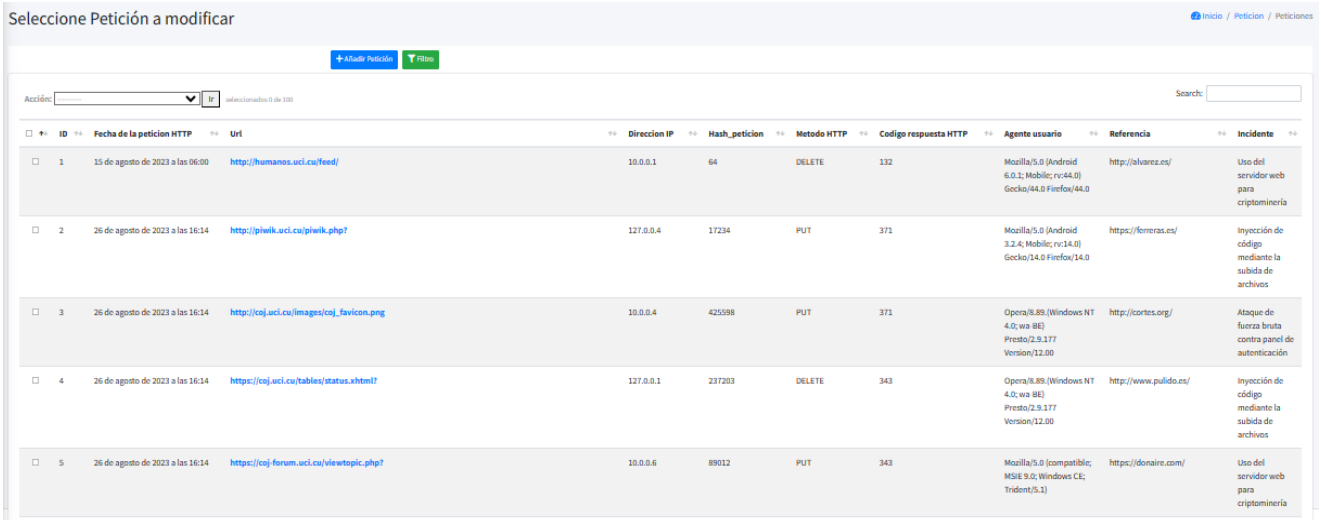

Seleccione Petición a modificar
Inicio / Peticion / Peticiones
+Añadir Petición
Filtro
Acción:
Ir
Search:
ID
Fecha de la peticion HTTP
Url
Direccion IP
Hash_peticion
Metodo HTTP
Codigo respuesta HTTP
Agente usuario
Referencia
Incidente
1 15 de agosto de 2023 a las 06:00 http://humanos.uci.cu/feed/ 10.0.0.1 64 DELETE 132 Mozilla/5.0 (Android 6.0.1; Mobile; rv:44.0) Gecko/44.0 Firefox/44.0 http://alvarez.es/ Uso del servidor web para criptominería
2 26 de agosto de 2023 a las 16:14 http://piwik.uci.cu/piwik.php? 127.0.0.4 17234 PUT 371 Mozilla/5.0 (Android 3.2.4; Mobile; rv:14.0) Gecko/14.0 Firefox/14.0 https://ferreras.es/ Inyección de código mediante la subida de archivos
3 26 de agosto de 2023 a las 16:14 http://coj.uci.cu/images/coj_favicon.png 10.0.0.4 425598 PUT 371 Opera/8.89.(Windows NT 4.0; wa IBE) Presto/2.9.177 Version/12.00 http://cortes.org/ Ataque de fuerza bruta contra panel de autenticación
4 26 de agosto de 2023 a las 16:14 https://coj.uci.cu/tables/status.xhtml? 127.0.0.1 237203 DELETE 343 Opera/8.89.(Windows NT 4.0; wa IBE) Presto/2.9.177 Version/12.00 http://www.pulido.es/ Inyección de código mediante la subida de archivos
5 26 de agosto de 2023 a las 16:14 https://coj-forum.uci.cu/viewtopic.php? 10.0.0.6 89012 PUT 343 Mozilla/5.0 (compatible; MSIE 9.0; Windows CE; Trident/5.1) https://donaire.com/ Uso del servidor web para criptominería

Tabla 6 Historia de Usuario #15

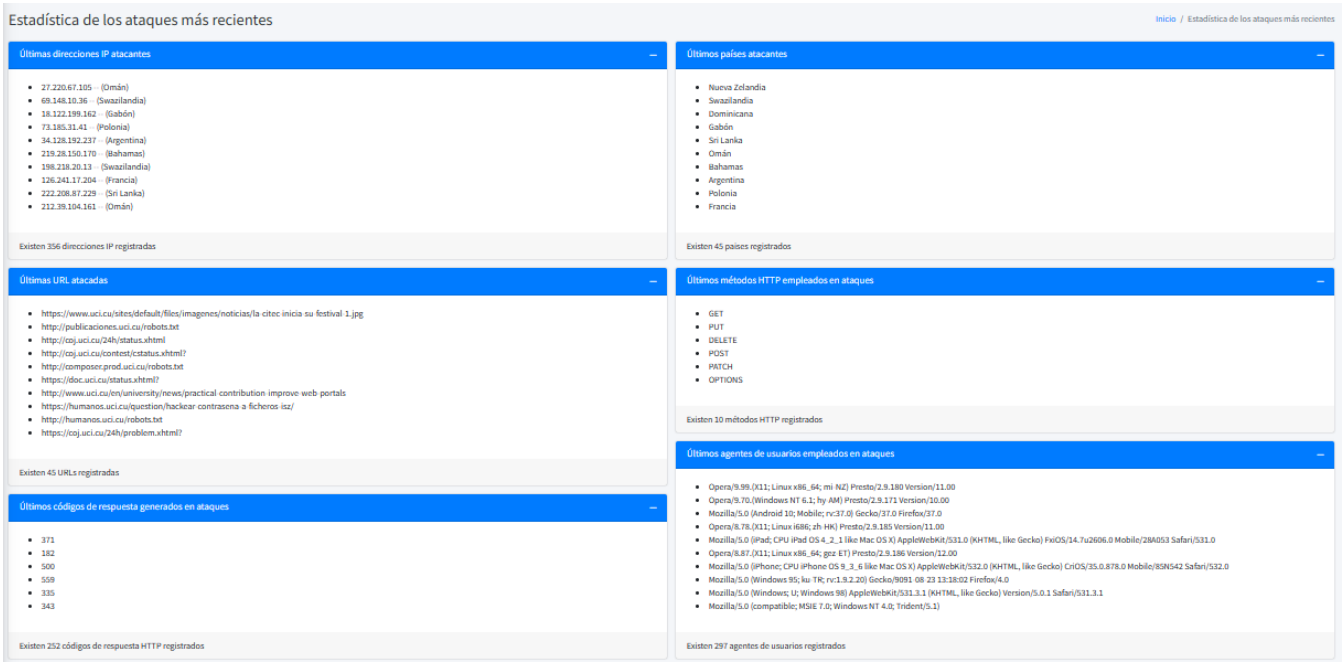
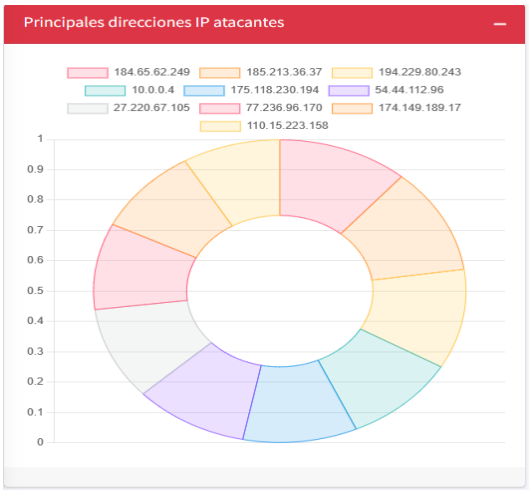
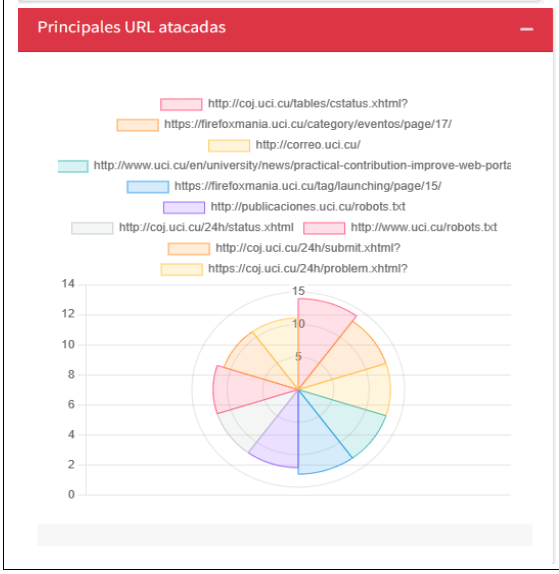
Historia de Usuario	
Número: HU_15	**Requisito:** Generar Reporte Ataques más recientes
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 2	**Iteración Asignada:** 2
Programador responsable: Yadira Sánchez Cruz	
Descripción: Permite que se realicen reportes de los últimos ataques efectuados, donde se muestra la siguiente información: • Últimas direcciones IP atacantes (muestra IP y país) • Últimos Países atacantes • Últimas URL atacadas • Últimos Métodos HTTP empleados en el ataque • Últimos códigos de respuestas generados en el ataque • Últimos agentes de usuarios empleados en el ataque	
Prototipo elemental de interfaz gráfica de usuario: 	

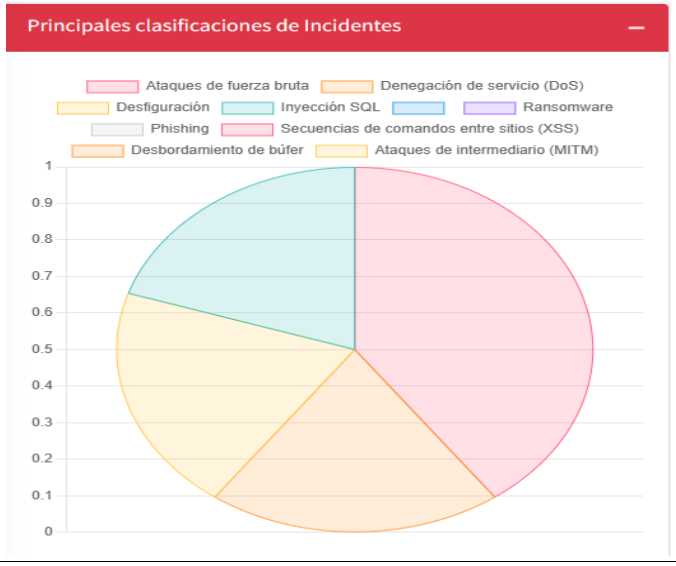
Tabla 7 Historia de Usuario #16

Historia de Usuario	
Número: HU_16	**Requisito:** Generar gráficos de Estadísticas Generales
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio

Puntos estimados: 2	**Iteración Asignada:** 2
Programador responsable: Yadira Sánchez Cruz	
Descripción: Permite que se realicen gráficos de estadísticas generes del sistema, donde se muestra la siguiente información: • Principales direcciones IP atacantes • Principales Países atacantes • Principales URL atacadas • Principales clasificaciones de incidentes • Principales tecnologías atacadas • Principales métodos HTTP empleados en el ataque	
Prototipo elemental de interfaz gráfica de usuario:	







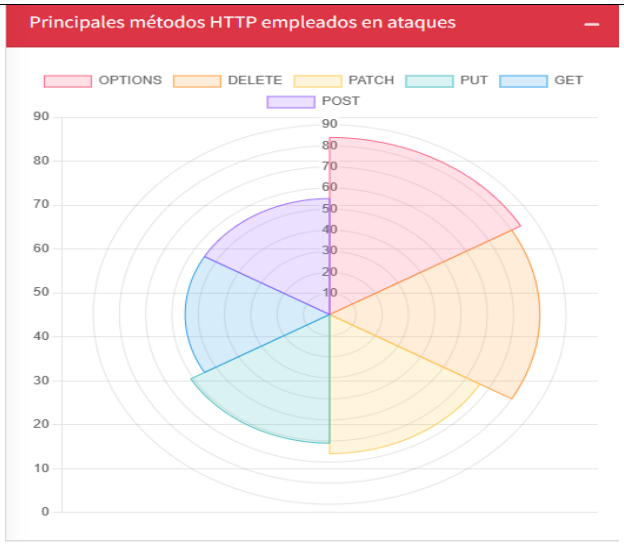
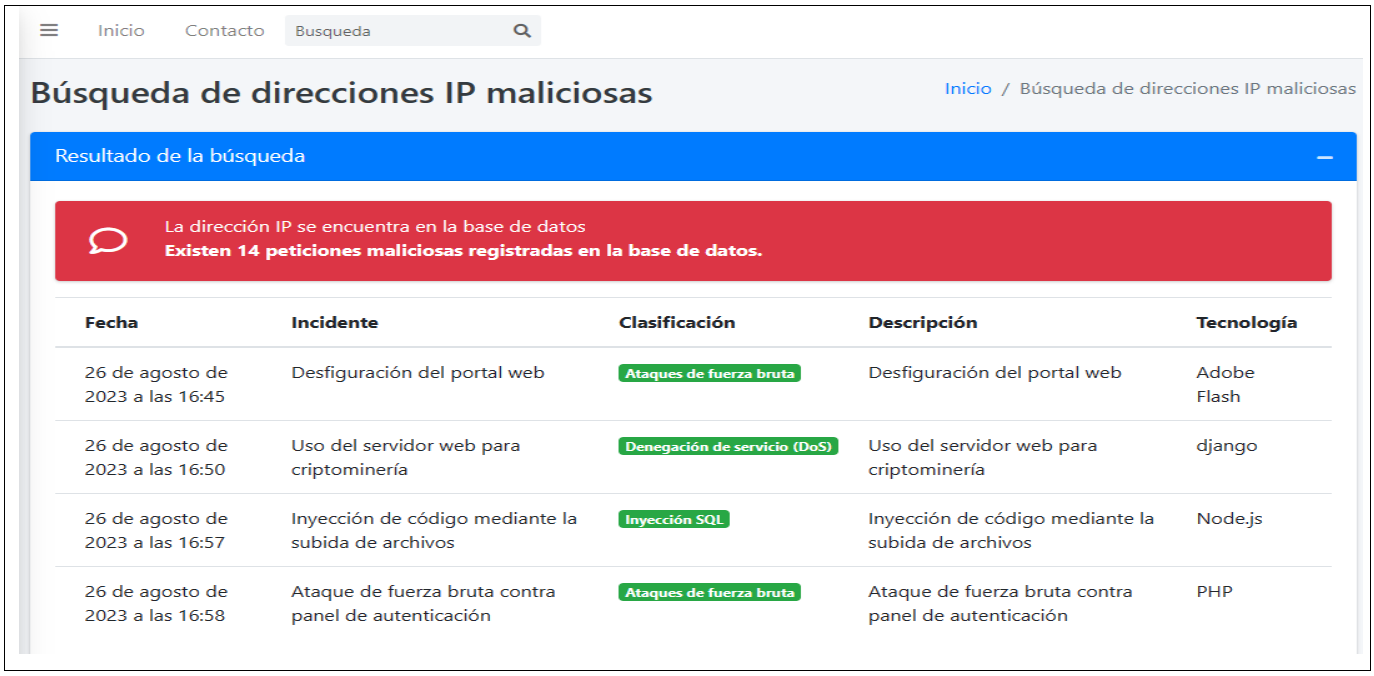


Tabla 8 Historia de Usuario #19

Historia de Usuario	
Número: HU_19	**Requisito:** Buscar número IP
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 0.3	**Iteración Asignada:** 2
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se permite al usuario buscar en la base de datos si existe un número IP determinado. • **buscar**: para ello, se teclea el número IP que se quiere buscar y como resultado se muestran todas las entradas en las que ha estado involucrado ese número IP (fecha en que intentó acceder, incidente reportado, clasificación del incidente, descripción del incidente y tecnología involucrada), además se muestra un mensaje de que la dirección IP se encuentra en la base de datos y la cantidad de peticiones registradas caso de no encontrarse la dirección IP se muestra que: “La dirección IP no se encuentra en la base de datos”	
Prototipo elemental de interfaz gráfica de usuario:	



Se puede consultar el resto de las historias de usuarios en el Anexo 1.

2.3.2 Estimación de esfuerzo por Historia de Usuario

Las estimaciones de esfuerzo asociado a la implementación de las HU la establecen los programadores utilizando como medida el punto de estimación. Un punto de estimación equivale a una semana de programación. Las HU generalmente valen de 1 a 3 puntos. Para una mayor organización se decide, además, asignar a cada iteración el conjunto de historias agrupadas en correspondencia con el tipo de HU a implementar, se establece una primera iteración donde se desarrollarán todos los CRUD y una segunda iteración dónde se desarrollarán los reportes:

Tabla 9 Estimación de esfuerzo por Historia de Usuario

Historias de Usuarios		Puntos Estimados (Semana)
HU 1	Gestionar País	0.3
HU 2	Gestionar Dirección IP	0.3
HU 3	Gestionar Método HTTP	0.3
HU 4	Gestionar Código de Respuesta HTTP	0.3
HU 5	Gestionar Agente de Usuario	0.3
HU 6	Gestionar Referencia	0.3
HU 7	Gestionar URL	0.3
HU 8	Gestionar Tecnología	0.3
HU 9	Gestionar Clasificación del Incidente	0.3
HU 10	Gestionar Entidades	0.3
HU 11	Gestionar Incidente	1.2
HU 12	Gestionar Peticiones	1.2

HU 13	Gestionar Grupo	0.3
HU 14	Gestionar Usuario	0.3
HU 15	Generar Reporte Ataques más recientes	2
HU 16	Generar gráficos de Estadísticas Generales	2
HU 17	Autenticar Usuario	0.3
HU 18	Datos de contacto	0.2
HU 19	Buscar número IP	0.3

2.3.3 Desarrollo del plan de iteraciones

Una vez definidas las HU y realizada una previa estimación de esfuerzos, se procede a la planificación de la etapa de implementación del sistema. En este espacio, se crea el plan de iteraciones, donde se especifica la prioridad con que se implementarán las HU organizadas por iteraciones. Teniendo en cuenta el esfuerzo asociado a las HU y a las prioridades del cliente, se define una versión que sea de valor para este.

Para el desarrollo de la propuesta se desarrollaron 2 iteraciones, las cuales fueron discutidas y aprobadas por el cliente, a continuación, se muestra el plan de iteraciones (Tabla 10)

2.3.4 Plan de duración de las iteraciones

A continuación, se presenta el plan de duración de las iteraciones. Este plan, tiene como finalidad, mostrar la duración de cada iteración, así como el orden en que serán implementadas las HU en cada iteración como se muestra en la tabla siguiente:

Tabla 10 Plan de duración de las Iteraciones

Iteración	Historia de Usuario	Duración (semanas)
1	HU 1 Gestionar País	3.0
	HU 2 Gestionar Dirección IP	
	HU 3 Gestionar Método HTTP	
	HU 4 Gestionar Código de Respuesta HTTP	
	HU 5 Gestionar Agente de Usuario	
	HU 6 Gestionar Referencia	
	HU 7 Gestionar URL	
	HU 8 Gestionar Tecnología	
	HU 9 Gestionar Clasificación del Incidente	
	HU 10 Gestionar Entidades	
2	HU 11 Gestionar Incidente	7.8
	HU 12 Gestionar Peticiones	
	HU 13 Gestionar Grupo	
	HU 14 Gestionar Usuario	

	HU 15 Generar Reporte Ataques más recientes	
	HU 16 Generar gráficos de Estadísticas Generales	
	HU 17 Autenticar Usuario	
	HU 18 Datos de contacto	
	HU 19 Buscar número IP	
Total		10.8

2.3.5 Plan de entregas

En el plan de entrega que se plantea a continuación, se hace una propuesta de las versiones (releases) del sistema. Cada versión se conformará al finalizar una iteración.

Tabla 11 Plan de entrega de versiones

Entregables	Iteración 1	Iteración 2
Módulos	Versión 1.0	Versión 1.1
Fecha	12/05/2023	24/06/2023

2.4 Fase II: Diseño del sistema

La metodología XP recomienda crear diseños simples y sencillos. Por esta razón, obtener un diseño que sea fácil de entender e implementar es un objetivo deseable para el equipo de desarrollo. Como resultado, en el futuro se reducirán los costos y el esfuerzo de los desarrolladores para mantener el sistema. En esta fase se estudian posibles opciones de implementación para el software que hay que construir, así como decidir la estructura general del mismo. El diseño es una etapa compleja y su proceso debe realizarse de manera iterativa.

2.4.1 Tarjetas CRC

Las HU son evaluadas para dividirlas en tareas, cada tarea representa una característica distinta del sistema y se puede diseñar una prueba de unidad que verifique cada tarea, estas tareas se representan por medio de las tarjetas Clase-Responsabilidad-Colaborador (CRC). Cada tarjeta contiene el nombre de la clase, una descripción de las responsabilidades o métodos asociados con la clase, así como la lista de las clases con que se relaciona o que colaboran con ella.

Teniendo en cuenta el uso del Django se definirán las clases Models y Admind con los métodos que se usarán y se heredarán por parte de las otras clases definidas en el proyecto. A continuación, se

describen las tarjetas definidas para la implementación de la solución. Se expondrán algunas en este apartado y las otras podrán consultarlas en los anexos del presente documento

Tabla 12 Tarjeta CRC # 1

Tarjeta CRC	
Clase: Models	
Responsabilidades	Colaboraciones
La clase modelo tiene la responsabilidad de definir las entidades de almacén de datos y las propiedades que se espera que tenga. Get () listar y mostrar Save () adicionar y modificar Delete () eliminar Filter () filtrar	

Tabla 13 Tarjeta CRC # 2

Tarjeta CRC	
Clase: Admin	
Responsabilidades	Colaboraciones
Construir automáticamente un área dentro del sitio que puedes usar para crear, consultar, actualizar y borrar registros List_display () listar y mostrar Add_field () adicionar y modificar Delete_field () eliminar Search_field () Buscar	Models

Tabla 14 Tarjeta CRC # 3

Tarjeta CRC	
Clase: Pais	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes a los países. Siendo una clase Modelo o también conocida como Entidad.	Models Admin PaisVisualizacion

Tabla 15 Tarjeta CRC # 8

Tarjeta CRC	
Clase: Incidente	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes al incidente ocurrido. Siendo una clase Modelo o también conocida como Entidad.	Models Tecnologia ClasificacionIncidente

	Entidad Admin IncidenteBuscador

Tabla 16 Tarjeta CRC # 14

Tarjeta CRC	
Clase: Peticion	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes a la petición realizada. Siendo una clase Modelo o también conocida como Entidad.	Models Admin DireccionIP MetodoHTTP CodigoRespuestaHTTP AgenteUsuario Referencia URL Incidente

Tabla 17 Tarjeta CRC # 15

Tarjeta CRC	
Clase: PaisVizualizacion	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar un país	Admin

Se puede consultar el resto de las Tarjetas CRC en el Anexo 2.

2.4.2 Patrón Arquitectónico

La arquitectura de software es la organización fundamental de un sistema enmarcada en sus componentes, las relaciones entre ellos, y el ambiente, y los principios que orientan su diseño y evolución. Al diseñar una arquitectura de software se crean y representan componentes que interactúan entre sí, con responsabilidades específicas y se organizan de forma tal que se logren los requerimientos establecidos. Se puede partir con patrones de soluciones probados que se conocen con el nombre de estilos arquitectónicos, patrones arquitectónicos y patrones de diseño (Rodríguez Peña and Silva Rojas 2016).

La propuesta de solución se implementó siguiendo los principios del patrón arquitectónico Modelo-Vista-Plantilla (MVT) utilizado por el framework Django para la representación de los proyectos. Se muestra que contendrá cada capa:

Modelo: Se encarga de gestionar los datos de las entidades de la base de datos. Esto puede incluir la creación, lectura, actualización y eliminación de las mismas, así como la gestión de los usuarios y sus permisos en la base de datos.

Vista: Se encarga de recibir las solicitudes de los usuarios, realizar las operaciones necesarias en el modelo y devolver una respuesta adecuada a través de las plantillas.

Plantilla: Se encarga de la presentación visual de los datos de la aplicación a los usuarios.

URLs: El mapeador URL se usa para redirigir las peticiones HTTP a la vista apropiada basándose en la URL de la petición

La figura 6. Muestra la vista arquitectónica del sistema.

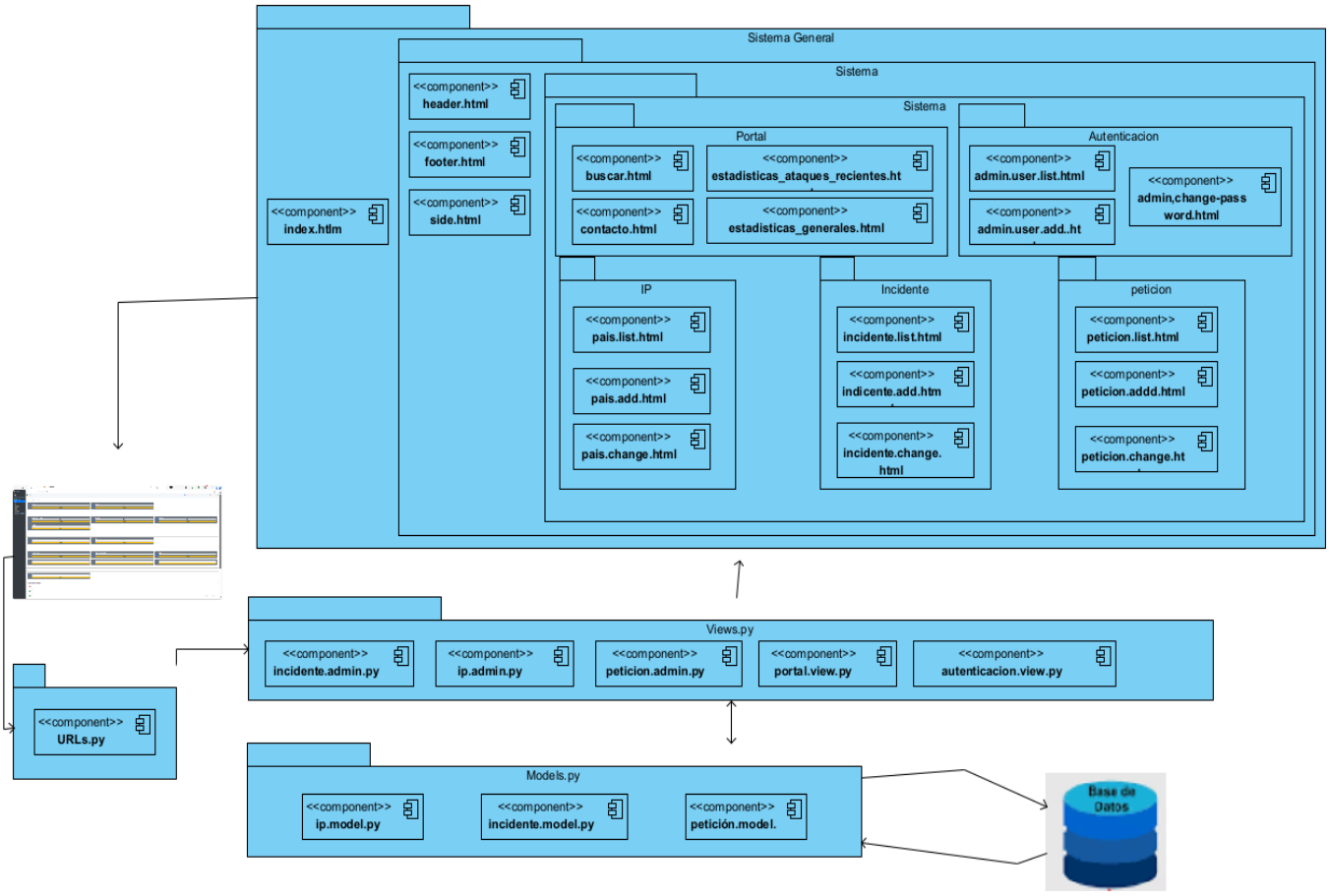


Figura 6 Vista del patrón arquitectónico MVT del sistema

Fuente: Elaboración Propia

2.4.3 Patrones de diseño

Los patrones de diseño, tratan los problemas que se repiten y que se presentan en situaciones particulares del diseño, con el fin de proponer soluciones a ellas. Se encargan de identificar clases, instancias, roles, colaboraciones entre estas, así como la distribución de responsabilidades (LARMAN, 2002). En resumen, es una descripción de clases y objetos comunicándose entre sí, adaptada para resolver un problema de diseño general en un contexto particular.

Para la asignación general de responsabilidades en el software existen patrones denominados Patrones Generales de Asignación de Responsabilidades (GRASP, por sus siglas en inglés), que describen los principios fundamentales de asignación de responsabilidades a objetos, expresadas como patrones. Seguidamente se exponen algunos patrones utilizados en muestro proyecto partiendo de que Django internamente implementa un grupo de estos patrones:

Experto: Es el encargado de asignar la responsabilidad de la creación de un objeto o la implementación de un método a una clase que contenga toda la información necesaria para cumplir con dicha responsabilidad (Pressman, 2005). En el proyecto presentado el models.py se encarga de la estructura de la base de datos y la lógica de la misma, por lo que es un ejemplo de este patrón.

Creador: El mismo tiene como objetivo asignar a la clase B la responsabilidad de crear una instancia de la clase A (Larman, 1999). Ejemplo del uso de este patrón en el proyecto lo tenemos en el admin.py es responsable de la creación de objetos de tipo model.

Bajo Acoplamiento: El acoplamiento es una medida de la fuerza con que una clase está conectada a otras clases, con qué las conoce y con qué concurre a ellas. En tal sentido, el término bajo acoplamiento significa que una clase no depende de muchas clases (Pressman, 2005). Ejemplo del uso de este patrón en el proyecto se encuentra las URL.py, las cuales llaman a funciones y métodos que implementan las Vistas, pero algún cambio que se realice a una función o método, no afecta la URL. Se puede decir que teniendo en cuenta la estructura del framework Django todas las clases definidas cumplen con este patrón.

Alta Cohesión: Es una medida de cuán relacionadas y enfocadas están las responsabilidades de una clase. Una alta cohesión caracteriza a las clases con responsabilidades estrechamente relacionadas que no realizan un trabajo enorme (Pressman, 2005). Ejemplo del uso de este patrón lo tenemos en las clases del modelo, las cuales describen la estructura de las tablas de la base de datos de manera coherente y precisa. Además, como en el patrón anterior podemos afirmar que todas las clases definidas cumplen con este patrón

Una vez definidos los patrones de diseño, se describen las clases utilizadas en la solución. Siguiendo la metodología XP, se analizan las HU y se descomponen en tareas independientes.

2.7 Conclusiones del capítulo

En este capítulo se han abordado los aspectos referentes a la concepción del producto a desarrollar y sus características funcionales. Esto permitió arribar a las siguientes conclusiones:

- A partir de la definición de las HU se pudieron identificar las principales funcionalidades a desarrollar en correspondencia con los módulos IP, Peticiones, Incidentes, Usuario y Reporte.
- La estimación del tiempo para la implementación de las HU definidas, permitió calcular una entrega final del producto en 10.8 semanas
- Fue posible identificar los patrones GRASP para el desarrollo de la solución propuesta.
- Se exponen los artefactos generados en las fases de Planificación y Diseño que establece la metodología XP.
- Con los aspectos arquitectónicos y de diseño a utilizar definidos, queda establecida la vía para llevar a cabo la implementación y prueba de los módulos.

CAPÍTULO III: IMPLEMENTACIÓN Y PRUEBA DE LA SOLUCIÓN PROPUESTA

En el presente capítulo se detallan las iteraciones realizadas durante la etapa de construcción de los módulos propuestos, además se exponen las tareas de ingeniería generadas para cada HU que fueron definidas, así como las pruebas de aceptación planificadas para el sistema. De esta forma es obtenido un producto funcional probado y listo para entregar al cliente al final de cada iteración como propone XP.

3.1 Fase III: Desarrollo

En esta fase, XP plantea que las HU seleccionadas para ser implementadas se realizan durante el transcurso de la iteración a la que pertenecen. Por estas razones, se lleva a cabo una revisión del plan de iteraciones y se modifican en caso de ser necesario. Como parte de este plan se descomponen las HU en tareas de ingeniería (JOSKOWICZ, 2008).

3.1.1 Tareas de Ingeniería

Las tareas de ingeniería pueden estar descritas por un lenguaje técnico y no ser necesariamente entendibles por el cliente. Tienen como objetivo definir cada una de las actividades que dan cumplimiento a las HU, de forma tal que se entienda lo que el sistema tiene que hacer y facilite su construcción. Se describen algunas de las tareas de ingeniería correspondientes a las HU del sistema, el resto pueden ser consultadas en los anexos. Para una mayor organización, se definen en correspondencia con las iteraciones definidas como se manifiesta a continuación.

Tareas de ingeniería para la Iteración I

Para la primera iteración, se definieron un total de 7 tareas de ingeniería. Todas, desglosadas a partir de las HU correspondientes a los módulos IP, Petición. Se describen algunas de las tareas realizadas en esta iteración.

Tabla 18 Tarea de ingeniería 1

Tarea de Ingeniería	
Número de la tarea: 1	**Número de Historia de Usuario:** 1
Nombre de la tarea: Visualización de los datos del país	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 06/03/2023	**Fecha de fin:** 08/03/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase Pais que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar un	

país

Tabla 19 Tarea de ingeniería 2

Tarea de Ingeniería	
Número de la tarea: 2	**Número de Historia de Usuario:** 2
Nombre de la tarea: Visualización de los datos de la dirección IP	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 09/03/2023	**Fecha de fin:** 13/03/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase DireccionIP que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar una dirección IP sospechosa	

Tabla 20 Tarea de ingeniería 3

Tarea de Ingeniería	
Número de la tarea: 3	**Número de Historia de Usuario:** 3
Nombre de la tarea: Visualización de los datos del método HTTP utilizado para realizar la petición sospechosa	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 14/03/2023	**Fecha de fin:** 16/03/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase MetodoHTTP que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar un método HTTP utilizado para realizar la petición sospechosa	

Tabla 21 Tarea de ingeniería 4

Tarea de Ingeniería	
Número de la tarea: 4	**Número de Historia de Usuario:** 4
Nombre de la tarea: Visualización de los datos del código de respuesta HTTP	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 20/03/2023	**Fecha de fin:** 22/03/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase CodigoRespuestaHTTP que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar un código de respuesta HTTP	

Nota: Las tareas de ingeniería correspondientes a las historias de usuarios que describen funcionalidades de adicionar, eliminar, modificar y buscar son realizadas por la clase admin.py del framework

Django que está diseñado para esta función, por lo que se decidió no describir estas tareas para no redundar información.

Tareas de ingeniería para la Iteración II

Para una segunda iteración, se elaboraron un total de 21 tareas de ingeniería. La mayoría, desglosadas a partir de las HU correspondientes a los módulos Incidente, Portal, Petición y Usuario. Se describen algunas de las tareas realizadas, el resto pueden ser consultadas en los anexos de la investigación.

Tabla 22 Tarea de ingeniería 12

Tarea de Ingeniería	
Número de la tarea: 12	**Número de Historia de Usuario:** 11
Nombre de la tarea: Visualización de los datos del incidente ocurrido	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.3
Fecha de inicio: 08/05/2023	Fecha de fin: 11/05/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase Incidente que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar del incidente ocurrido, así como filtrar por los datos que se muestran.	

Tabla 23 Tarea de ingeniería 13

Tarea de Ingeniería	
Número de la tarea: 13	**Número de Historia de Usuario:** 12
Nombre de la tarea: Visualización de los datos de la petición sospechosa	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.3
Fecha de inicio: 15/03/2023	**Fecha de fin:** 18/05/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase Peticion que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar de la petición sospechosa realizada, así como filtrar por los datos que se muestran.	

Tabla 24 Tarea de ingeniería 14

Tarea de Ingeniería	
Número de la tarea: 14	**Número de Historia de Usuario:** 15
Nombre de la tarea: Visualizar reporte de las últimas IP atacantes	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 22/05/2023	**Fecha de fin:** 24/05/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción:	

Se implementa una funcionalidad que permite mostrar las últimas 10 IP atacantes registradas en el sistema, mostrando una lista con las direcciones IP que hayan sido insertadas en los últimos días

Tabla 25 Tarea de ingeniería 20

Tarea de Ingeniería	
Número de la tarea: 20	**Número de Historia de Usuario:** 16
Nombre de la tarea: Generar gráfico de principales direcciones IP atacantes	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 14/06/2023	**Fecha de fin:** 15/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite generar un gráfico donde se muestre cuáles han sido las principales direcciones IP atacantes, teniendo en cuenta el nivel de peligrosidad del incidente causado.	

Tabla 26 Tarea de ingeniería 21

Tarea de Ingeniería	
Número de la tarea: 21	**Número de Historia de Usuario:** 16
Nombre de la tarea: Generar gráfico de los principales países atacantes	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 19/06/2023	**Fecha de fin:** 20/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite generar un gráfico donde se muestre cuáles han sido los principales países atacantes, teniendo en cuenta la cantidad de veces que han realizado peticiones sospechosas.	

Tabla 27 Tarea de ingeniería 28

Tarea de Ingeniería	
Número de la tarea: 28	**Número de Historia de Usuario:** 19
Nombre de la tarea: Buscar un Número IP en la base de datos	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.3
Fecha de inicio: 19/06/2023	**Fecha de fin:** 22/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite introducir un número IP y el sistema verifica y si está en la base de Datos muestra los datos asociados a dicho número IP (incidentes, fechas, descripción, peticiones)	

Tabla 28 Tarea de ingeniería 29

Tarea de Ingeniería	
Número de la tarea: 29	**Número de Historia de Usuario:** Todas
Nombre de la tarea: Diseñar e implementar front end de la aplicación	
Tipo de tarea: Desarrollo	**Puntos estimados:** 2
Fecha de inicio: 14/04/2023	**Fecha de fin:** 22/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite desarrollar con HTML, CSS y JavaScript la interfaz de usuario para que sea posible la interacción con el sistema.	

Nota: El gestionar grupo y usuario correspondiente a las HU 13 y 14 se hace desde las mismas clases que provee el framework Django para esas funciones, por lo que no es necesario definir tareas de ingeniería para ello.

Se puede consultar el resto de las tareas de ingeniería en el Anexo 3.

Con las tareas de ingeniería definidas, se hace necesario establecer un conjunto de pruebas para comprobar la calidad de la solución implementada. Luego, se analizan estos casos de prueba y se ejecutan, lo que permite medir el nivel de cumplimiento con los objetivos de implementación trazados y el nivel de satisfacción del cliente. Así lo propone XP.

3.2 Fase IV: Pruebas

Las pruebas son un conjunto de actividades que se pueden planificar por adelantado y llevar a cabo sistemáticamente. Por esta razón, se deben definir en el proceso de la ingeniería del software. Todo esto, contribuye a elevar la calidad de los productos desarrollados y a la seguridad de los programadores a la hora de introducir cambios o modificaciones.

La metodología XP divide las pruebas en dos grupos: pruebas unitarias, desarrolladas por los programadores, encargadas de verificar el código de forma automática y las pruebas de aceptación, destinadas a evaluar si al final de una iteración se obtuvo la funcionalidad requerida, además de comprobar que dicha funcionalidad sea la esperada por el cliente (ESCRIBANO, 2002).

Se decide realizar las pruebas de aceptación a los módulos implementados, debido a que el objetivo de estas, es verificar que el sistema cumpla con los requisitos establecidos por el usuario. De esta forma se puede obtener el grado de satisfacción del cliente, además el cliente abogó por este tipo de pruebas.

Se decidió que como pate del proceso de pruebas además se realizaran pruebas funcionales al sistema, estas pruebas se realizaron haciendo uso de los mismos casos de pruebas definidos para las

pruebas de aceptación, pues los mismos se diseñaron de manera que se probaran las funcionalidades del sistema.

3.2.1. Pruebas de aceptación

Las pruebas de aceptación son especificadas por el cliente, se centran en las características y funcionalidades generales del sistema que son visibles. Estas pruebas derivan de las HU que se han implementado como parte de la liberación del software. Una prueba de aceptación es como una caja negra. Cada una de ellas representa una salida esperada del sistema. Es responsabilidad del cliente verificar la corrección y toma de decisiones acerca de estas pruebas. A continuación, se muestra una representación de las pruebas de aceptación a realizarse en cada iteración.

3.2.2. Pruebas de aceptación para la iteración 1

Para la primera iteración, se definieron un total de 30 casos de pruebas, enfocadas a evaluar la implementación de los módulos IP e Incidente. Se describen algunas de las pruebas realizadas, el resto pueden ser consultadas en el Anexos 4 de la investigación.

Tabla 29 Prueba de Aceptación 1

Caso de prueba de aceptación	
Código: HU1_P1	**Historia de usuario:** 1
Nombre: Adicionar un País	
Descripción: Prueba para la funcionalidad Gestionar país, en este caso para Adicionar país (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El país no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*IP'* 2. El usuario selecciona dentro de las opciones del módulo IP la opción '*Países*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de un país. 3. El usuario selecciona dentro de la vista el botón '*Anadir País*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del país 4. El usuario completa el campo 'Nombre 'en el formulario, este dato es una cadena de caracteres de longitud 50 y selecciona cualquiera de los tres botones que aparecen en el formulario: a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de países con el país agregado al final de la lista b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó el país correctamente y se mantiene en el formulario para poder adicionar un nuevo país c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó el país correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar el país	
Evaluación de la prueba: Satisfactoria	

Tabla 30 Prueba de Aceptación 2

Caso de prueba de aceptación	
Código: HU1_P2	**Historia de usuario:** 1
Nombre: Adicionar un País	
Descripción: Prueba para la funcionalidad Gestionar país, en este caso para Adicionar país (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El país no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*IP'* 2. El usuario selecciona dentro de las opciones del módulo IP la opción '*Países*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de un país. 3. El usuario selecciona dentro de la vista el botón '*Anadir País*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del país 4. El usuario completa el campo 'Nombre 'en el formulario introduciendo el nombre de un país que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 5. El sistema muestra mensajes de error de ya existe un país con ese nombre o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 31 Prueba de Aceptación 3

Caso de prueba de aceptación	
Código: HU1_P3	**Historia de usuario:** 1
Nombre: Modificar un País	
Descripción: Prueba para la funcionalidad Gestionar país, en este caso para Modificar un país	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El país debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*IP'* 2. El usuario selecciona dentro de las opciones del módulo IP la opción '*Países*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de un país. 3. El usuario debe pinchar sobre el nombre del país que quiere modificar y el sistema debe llevarlo a la vista de Adicionar país, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar el país 4. El usuario modifica el campo 'Nombre 'en el formulario, este dato es una cadena de caracteres de longitud 50 y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de países con el país agregado al final de la lista y un mensaje diciendo que el país fue modificado correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió el país correctamente y se mantiene en el formulario para poder adicionar un nuevo país c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió el país correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar el país d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados al país que se quiere eliminar y da dos opciones (si quiere eliminar el país, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 32 Prueba de Aceptación 4

Caso de prueba de aceptación	
Código: HU12_P1	**Historia de usuario:** 12
Nombre: Adicionar una petición	
Descripción: Prueba para la funcionalidad Gestionar Petición, en este caso para Adicionar una petición (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La petición no debe verse adicionado anteriormente	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Peticiones*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la petición. 3. El usuario selecciona dentro de la vista el botón '*Anadir Petición*, el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la petición 4. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 112 y selecciona cualquiera de los tres botones que aparecen en el formulario: a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de peticiones con la petición agregada al final de la lista b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó la petición correctamente y se mantiene en el formulario para poder adicionar una nueva petición c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó la petición correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la petición	
Evaluación de la prueba: Satisfactoria	

Tabla 33 Prueba de Aceptación 5

Caso de prueba de aceptación	
Código: HU1_P5	**Historia de usuario:** 1
Nombre: Buscar un País	
Descripción: Prueba para la funcionalidad Gestionar país, en este caso para Buscar un país	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El país debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*IP'* 2. El usuario selecciona dentro de las opciones del módulo IP la opción '*Países*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de un país. 3. El usuario escribe el nombre del país que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con el país seleccionado, en caso de no encontrarse debe mostrar el mensaje de que el país no fue encontrado	
Evaluación de la prueba: Satisfactoria	

3.2.3. Pruebas de aceptación para la iteración 2

Para la primera iteración, se definieron un total de 40 casos de pruebas de aceptación, enfocadas a evaluar la implementación de los módulos petición y usuario. Se describen algunas de las pruebas realizadas, el resto pueden ser consultadas en los anexos de la investigación.

Tabla 34 Prueba de Aceptación 56

Caso de prueba de aceptación	
Código: HU12_P2	**Historia de usuario:** 12
Nombre: Adicionar petición	
Descripción: Prueba para la funcionalidad Gestionar Petición, en este caso para Adicionar petición (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La petición no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Peticiones*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la petición. 3. El usuario selecciona dentro de la vista el botón '*Anadir Petición*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la petición 4. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de una petición que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 5. El sistema muestra mensajes de error de ya existe una petición con esa descripción o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 35 Prueba de Aceptación 57

Caso de prueba de aceptación	
Código: HU12_P3	**Historia de usuario:** 12
Nombre: Modificar una petición	
Descripción: Prueba para la funcionalidad Gestionar Petición, en este caso para Modificar una petición	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La petición debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Peticiones*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la petición. 3. El usuario debe pinchar sobre la petición que quiere modificar y el sistema debe llevarlo a la vista de Adicionar petición, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar la petición 4. El usuario modifica el campo 'descripción 'en el formulario, este dato debe ser una cadena de caracteres y aceptar hasta 112 caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de os peticiones con la petición agregado al final de la lista y un mensaje diciendo que la petición fue modificada correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió la petición correctamente y se mantiene en el formulario para poder adicionar una nueva petición c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió la petición correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la petición d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados a la petición que se quiere eliminar y da dos opciones (si quiere eliminar la petición, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 36 Prueba de Aceptación 58

Caso de prueba de aceptación	
Código: HU12_P4	**Historia de usuario:** 12
Nombre: Eliminar petición	
Descripción: Prueba para la funcionalidad Gestionar Petición, en este caso para eliminar una petición	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La petición debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Peticiones*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la petición. 3. El usuario selecciona la petición que quiere eliminar marcando el cuadro que aparece delante del identificador, busca la acción eliminar petición seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados al petición y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina la petición con todos los elementos asociados a él y muestra el mensaje se eliminó 1 Petición satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de las peticiones	
Evaluación de la prueba: Satisfactoria	

Tabla 37 Prueba de Aceptación 59

Caso de prueba de aceptación	
Código: HU12_P5	**Historia de usuario:** 12
Nombre: Buscar petición	
Descripción: Prueba para la funcionalidad Gestionar Petición, en este caso para Buscar una petición	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La petición debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Peticiones*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la petición. 3. El usuario escribe la descripción de la petición que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con la petición seleccionado, en caso de no encontrarse debe mostrar el mensaje de que la petición no fue encontrada	
Evaluación de la prueba: Satisfactoria	

3.2.4. Pruebas de aceptación para la iteración 3

Para la primera iteración, se definieron un total de 5 casos de pruebas de aceptación, enfocadas a evaluar la implementación del módulo Portal. Se describen algunas de las pruebas realizadas, el resto pueden ser consultadas en los anexos de la investigación.

Tabla 38 Prueba de Aceptación 71

Caso de prueba de aceptación	
Código: HU15_P1	**Historia de usuario:** 15
Nombre: Mostrar reportes de estadística reciente.	
Descripción: Prueba para la funcionalidad Generar Reporte Ataques más recientes, en este caso para mostrar los reportes.	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema	
Pasos de ejecución: 5. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Portal'* 6. El usuario selecciona la opción 'Reportes'. 7. El usuario selecciona dentro de la opción 'Reportes', la opción Ataques más Recientes 8. El sistema debe mostrar en el panel derecho una vista que permite ver los reportes	
Evaluación de la prueba: Satisfactoria	

Tabla 39 Prueba de Aceptación 72

Caso de prueba de aceptación	
Código: HU16_P1	**Historia de usuario:** 16
Nombre: Mostrar estadísticas generales.	
Descripción: Prueba para la funcionalidad Generar gráficos de Estadísticas Generales, en este caso para mostrar gráficos con estadísticas generales.	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Portal'* 2. El usuario selecciona la opción 'Reportes'. 3. El usuario selecciona dentro de la opción 'Reportes', la opción Estadísticas generales 4. El sistema debe mostrar en el panel derecho una vista que permite ver los gráficos con las estadísticas generales	
Evaluación de la prueba: Satisfactoria	

3.2.5. Análisis de las pruebas de funcionalidad y aceptación

Hasta el momento se han desarrollado un total de 75 casos de pruebas. Estas pruebas fueron realizadas de forma organizada, por cada iteración definida. A continuación, se muestra en gráficas, figura 7, los porcientos de satisfacción alcanzados en cada iteración:

Figura 7 Resultados de las pruebas de aceptación

Como se puede observar en la representación, en la primera iteración se realizaron un total de 30 pruebas, de ellas 27 alcanzaron el nivel de satisfacción esperado alcanzando un 90 %, mientras que en 3 de las pruebas se detectó que el sistema no especificaba que se había adicionado el elemento correctamente. Lo que permitió corregir la falla, e incorporar la validación de esta operación en el sistema.

En la iteración 2 se realizaron 40 pruebas, de ellas 39 alcanzaron el nivel de satisfacción esperado alcanzando un 97%, mientras que en 1 prueba se detectó que el sistema permitía entrar números en el campo descripción de la petición en la opción adicionar petición, esto permitió corregir y validar dicho campo a tiempo.

En la iteración 3, se realizaron 5 pruebas respectivamente, donde todas son evaluadas de resultado satisfactorio. Además, se probaron nuevamente las pruebas que habían salido erróneas en las iteraciones anteriores con el objetivo de verificar que realmente se cumple con todos los requisitos del sistema Con estas comprobaciones, se obtiene un 100 % de satisfacción en la iteración final del producto, comprobando el correcto funcionamiento de las funcionalidades implementadas. El cliente mostró su satisfacción con el sistema lo que se muestra en el aval de conformidad presentado como parte de dicha investigación.

3.3 Conclusiones del capítulo

En este capítulo se especificó el proceso de implementación del sistema a partir del desglose de las HU en tareas de ingeniería, lo que permitió especificar los procedimientos necesarios para dar cumplimiento a cada HU. Además, se definieron y aplicaron las pruebas de aceptación a las funcionalidades de los módulos desarrollados. Estas pruebas permitieron detectar 4 falla en el sistema y corregirla lo que posibilitó mejorar la operabilidad del mismo.

CONCLUSIONES FINALES

Con el desarrollo de la presente investigación se arriba a las siguientes conclusiones:

- Se logró establecer los fundamentos y referentes teórico-metodológicos para el desarrollo de un sistema informático para la detección de escaneos en Sistemas de Gestión de Contenidos Web quedando evidenciado la carencia de un sistema de este tipo en el país, así como la importancia de contar con uno propio.
- El diagnóstico realizado del estado actual del proceso detección de escaneos en Sistemas de Gestión de Contenidos Web arrojó un conjunto de deficiencias que alzaron la importancia de contar con un sistema de este tipo en el país.
- La utilización de las tecnologías y herramientas definidas permitió que la solución informática desarrollada sea un referente para el país, obteniendo un sistema que mejorará la seguridad de los Sistemas de Gestión de Contenidos Web, brindando una lista de IP sospechosas. Por su importancia forma parte de un proyecto del grupo de investigación de Ciberseguridad de la UCI.
- Se Implementó un API REST de manera adicional para facilitar la comunicación entre los sistemas que quieran consumir los servicios del sistema propuesto de manera que la usabilidad del mismo sea amplia y sencilla.
- Las pruebas de aceptación realizadas al software implementado demostraron el cumplimiento de los atributos de calidad, lo que se demuestra en el resultado obtenido por las mismas en la evaluación de los módulos del sistema, los cuales cumple satisfactoriamente con los requisitos definidos por los clientes.

RECOMENDACIONES

A partir de los resultados obtenidos se recomienda:

- Para versiones futuras de la aplicación incluir técnicas de Inteligencia Artificial y Aprendizaje Automático para automatizar la gestión de las trazas y garantizar que el sistema aprenda a identificar automáticamente las trazar sospechosas.

REFERENCIAS BIBLIOGRÁFICAS

AbuseIPDB. (s.f.). AbuseIPDB - IP Abuse Reports Database. [Sitio web]. Recuperado de https://www.abuseipdb.com/

Ahlawat, S., Tudu, J., Gaur, M. S., Fujita, M., y Singh, V. (2019). Preventing scan attack through test response encryption. Paper presented at the 2019 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT).

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., y Ahmad, F. J. T. o. E. T. T. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. 32(1), e4150.

Akiyama, M., Yagi, T., Yada, T., Mori, T., y Kadobayashi, Y. (2017). Analyzing the ecosystem of malicious URL redirection through longitudinal observation from honeypots. Computers y Security, 69, 155-173.

Ali, A. J. I. J. o. a. h. R. (2022). Cyberspace and Organized Crime: The New Challenges of the 21st Century. 2(1), 22-37.

Boehm, B., y Turner, R. (2003). Observations on Balancing Discipline and Agility. Recuperado de IEEE Xplore 2003: http://ieeexplore.ieee.org/xpl/mostRec entIssue.jsp?punumber=8714

Bridges, R. A., Glass-Vanderlan, T. R., Iannacone, M. D., Vincent, M. S., y Chen, Q. J. A. C. S. (2019). A survey of intrusion detection systems leveraging host data. 52(6), 1-35.

Calzavara, S., Focardi, R., Squarcina, M., y Tempesta, M. (2017). Surviving the Web: A Journey into Web Session Security. ACM Computing Surveys, 50(1), 13.

Consejo_de_Ministros. (2019). Decreto No. 360 sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional.

Dawamsyach, F., Ruslianto, I., y Ristian, U. J. C. Implementation of IPS (Intrusion Prevention System) Fail2ban on Server for DDoS and Brute Force Attacks. 8(1), 149-161.

Dhanya, K. A., Vajipayajula, S., Srinivasan, K., Tibrewal, A., Kumar, T. S., y Kumar, T. G. (2023). Detection of Network Attacks using Machine Learning and Deep Learning Models. 218(C %J Procedia Comput. Sci.), 57–66. doi: 10.1016/j.procs.2022.12.401

Dong, Y., Zhang, Y., Ma, H., Wu, Q., Liu, Q., Wang, K., y Wang, W. (2018). An adaptive system for detecting malicious queries in web attacks. Science China Information Sciences, 61(3), 032-114.

Duckett, J. (2011). HTML and CSS: Design and Build Websites. Wiley.

Escribano, G. 2002. Introducción a Extreme Programming. Introducción a Extreme Programming. 2002.

Flanagan, D. (2020). JavaScript: The Definitive Guide (7th ed.). O'Reilly Media.

Franklin, J., Wergin, C., y Booth, H. (2014). CVSS implementation guidance. National Institute of Standards and Technology, NISTIR-7946.

González Brito, H. R., y Montesino Perurena, R. J. R. C. d. C. I. (2018). Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. 12(4), 52-65.

Huang, H. C., Zhang, Z. K., Cheng, H. W., y Shieh, S. W. (2017). Web Application Security: Threats, Countermeasures, and Pitfalls. Computer, 50(6), 81-85. doi:10.1109/MC.2017.183

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., Mahmood, S. J. A. J. f. S., y Engineering. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. 45, 3171-3189.

Imeri, A., y Rysavy, O. (2023). Deep learning for predictive alerting and cyber-attack mitigation. Paper presented at the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC).

Jagamogan, R. S., Ismail, S. A., Hafizah, N., y Abas, H. H. (2021). A review: Penetration testing approaches on content management system (cms). Paper presented at the 2021 7th International Conference on Research and Innovation in Information Systems (ICRIIS).

Jana, I., y Oprea, A. (2019). AppMine: Behavioral analytics for web application vulnerability detection. Paper presented at the Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop.

Jang, S., Woo, H., Kim, S., y Kang, S. (2021). Secure Scan Design through Pseudo Fault Injection. Paper presented at the 2021 18th International SoC Design Conference (ISOCC).

JetBrains. (2021). PyCharm Community Edition (Version 2021.3). [Software]. Available from https://www.jetbrains.com/pycharm/

Kasturi, R. P., Sun, Y., Duan, R., Alrawi, O., Asdar, E., Zhu, V., . . . Saltaformaggio, B. (2020). TARDIS: Rolling back the clock on CMS-targeting cyber attacks. Paper presented at the 2020 IEEE Symposium on Security and Privacy (SP).

Kim, A., Park, M., y Lee, D. H. J. I. A. (2020). AI-IDS: Application of deep learning to real-time Web intrusion detection. 8, 70245-70261.

Kissel, R. (2019). NIST IR 7298 Glossary of key information security terms. 2, 10-38.

Kozik, R., Choraś, M., Renk, R., y Hołubowicz, W. (2014, 2014//). Modelling HTTP Requests with Regular Expressions for Detection of Cyber Attacks Targeted at Web Applications. Paper presented at the International Joint Conference SOCO'14-CISIS'14-ICEUTE'14, Cham.

Kumar, A., y Lim, T. J. (2019). EDIMA: Early detection of IoT malware network activity using machine learning techniques. Paper presented at the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT).

Lala, S. K., Kumar, A., y Subbulakshmi, T. (2021). Secure web development using owasp guidelines. Paper presented at the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS).

Li, Y., y Liu, Q. J. E. R. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. 7, 8176-8186.

Li, Y., y Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186. doi:https://doi.org/10.1016/j.egyr.2021.08.126

Maida, E. G., y Pacienzia, J. (2015). Metodologías de desarrollo de software. https://repositorio.uca.edu.ar/handle/123456789/522

Mansfield-Devine, S. (2017). Open source software: determining the real risk posed by vulnerabilities. Network Security, 2017(1), 7-12.

MariaDB Foundation. (2022). MariaDB: The Open Source Database for Developers. [Software]. Available from https://mariadb.org/

Martínez, S., Cosentino, V., y Cabot, J. (2017). Model-based analysis of Java EE web security misconfigurations. Computer Languages, Systems y Structures, 49, 36-61.

Mazurczyk, W., y Caviglione, L. J. C. o. t. A. (2021). Cyber reconnaissance techniques. 64(3), 86-95.

Meyer, E., y Lea, V. B. (2020). CSS: The Definitive Guide: Visual Presentation for the Web (4th ed.). O'Reilly Media.

Microsoft Corporation. (2022). Visual Studio Code: Code Editing. Redefined. [Software]. Available from https://code.visualstudio.com/

Microsoft Corporation. (2022). SQL Server (Version 2019). [Software]. Available from https://www.microsoft.com/en-us/sql-server

MongoDB Inc. (2022). MongoDB: The Modern Database for Modern Applications. [Software]. Available from https://www.mongodb.com/

Morrison, P., Smith, B. H., y Williams, L. (2017). Surveying Security Practice Adherence in Software Development. Paper presented at the Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp, Hanover, MD, USA.

Naik, N., Jenkins, P., Grace, P., y Song, J. (2022). Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATTyCK Framework and Diamond Model. Paper presented at the 2022 IEEE International Symposium on Systems Engineering (ISSE).

Nair, D., y Mhavan, N. (2023). Augmenting Cybersecurity: A Survey of Intrusion Detection Systems in Combating Zero-day Vulnerabilities. In Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy (pp. 129-153): Emerald Publishing Limited.

OSSEC. (2022). OSSEC: Open Source HIDS. [Software]. Available from https://www.ossec.net/

Patel, K. (2019, 23-25 April 2019). A Survey on Vulnerability Assessment y Penetration Testing for Secure Communication. Paper presented at the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI).

Roesch, M. (2015). Snort Intrusion Detection System (Version 2.9.15). [Software]. Available from https://www.snort.org/

Roesch, M., y Markoff, J. (2010). The Suricata Engine: Fast and Scalable Intrusion Detection (Version 6.0.2) [Software]. Available from https://suricata-ids.org/

Saputra, I. P., Utami, E., y Muhammad, A. H. (2022). Comparison of anomaly based and signature based methods in detection of scanning vulnerability. Paper presented at the 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI).

Seacord, R. C. (2017, 24-26 Sept. 2017). Java Deserialization Vulnerabilities and Mitigations. Paper presented at the 2017 IEEE Cybersecurity Development (SecDev).

Shahid, W. B., Aslam, B., Abbas, H., Afzal, H., Khalid, S. B. J. J. o. I. S., y Applications. (2022). A deep learning assisted personalized deception system for countering web application attacks. 67, 103169.

Shugrue, D. (2017). Fighting application threats with cloud-based WAFs. Network Security, 2017(6), 5-8.

Špaček, S., Laštovička, M., Horák, M., y Plesník, T. (2019). Current issues of malicious domains blocking. Paper presented at the 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM).

Soliman, K., Sobh, M. A., y Bahaa-Eldin, A. M. (2021). Survey of Machine Learning HIDS Techniques. Paper presented at the 2021 16th International Conference on Computer Engineering and Systems (ICCES).

Šuľan, S., y Husák, M. (2022). Limiting the Size of a Predictive Blacklist While Maintaining Sufficient Accuracy. Paper presented at the Proceedings of the 17th International Conference on Availability, Reliability and Security.

Sureda Riera, T., Bermejo Higuera, J.-R., Bermejo Higuera, J., Martínez Herraiz, J.-J., y Sicilia Montalvo, J.-A. J. S. (2020). Prevention and fighting against web attacks through anomaly detection technology. A systematic review. 12(12), 4945.

Thakkar, A., y Lohiya, R. J. A. I. R. (2022). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. 55(1), 453-563.

The Django Software Foundation. (2020). Django documentation: Version 3.1. Django Software Foundation. https://docs.djangoproject.com/en/3.1/

The PostgreSQL Global Development Group. (2021). PostgreSQL 14 Documentation. [Software]. Available from https://www.postgresql.org/docs/14/

Van Rossum, G., y Drake, F. L. (2021). Python 3 Reference Manual: Python Documentation (Vol. 3.10.0rc2). Python Software Foundation

Visual Paradigm International. (2021). Visual Paradigm: A Practical Guide to UML Modeling and Beyond (Version 16.3). Visual Paradigm International.

Wang, R., Xu, G., Zeng, X., Li, X., y Feng, Z. (2017). TT-XSS: A novel taint tracking based dynamic detection framework for DOM Cross-Site Scripting. Journal of Parallel and Distributed Computing.

Wazuh Inc. (2022). Wazuh: Open Source Host and Endpoint Security Solutions. [Software]. Available from https://wazuh.com/

Wickramasinghe, N., Nabeel, M., Thilakaratne, K., Keppitiyagama, C., y De Zoysa, K. J. a. p. a. (2021). Uncovering IP address hosting types behind malicious websites.

Woo, H., Jang, S., y Kang, S. (2021). A Secure Scan Architecture Protecting Scan Test and Scan Dump Using Skew-Based Lock and Key. IEEE Access, 9, 102161-102176. doi:10.1109/ACCESS.2021.3097348

Yánez Triana, C. K. (2022). Estudio comparativo de las herramientas de metodologías ágiles para el aplicar buenas prácticas de desarrollo en la calidad de software. [BachelorThesis, Babahoyo: UTB-FAFI. 2022]. http://dspace.utb.edu.ec/handle/49000/11852

Yuan, H., Zheng, L., Dong, L., Peng, X., Zhuang, Y., y Deng, G. (2019). Research and implementation of WEB application firewall based on feature matching. Paper presented at the Application of Intelligent Systems in Multi-modal Information Analytics.

ANEXOS

Anexo 1. Historias de usuarios

Tabla 40 Historia de Usuario #2

<table>
<tr><td colspan="3">Historia de Usuario</td></tr>
<tr><td>Número: HU_2</td><td colspan="2">Requisito: Gestionar Dirección IP</td></tr>
<tr><td colspan="3">Usuario: Administrador</td></tr>
<tr><td colspan="2">Prioridad en el negocio: Alta</td><td>Riesgo en Desarrollo: Medio</td></tr>
<tr><td colspan="2">Puntos estimados: 0.3</td><td>Iteración Asignada: 1</td></tr>
<tr><td colspan="3">Programador responsable: Yadira Sánchez Cruz</td></tr>
<tr><td colspan="3">Descripción: El administrador requiere gestionar los datos de las direcciones IP por las cuales se han realizado peticiones sospechosas, para lo cual se muestra una lista de las mismas con el identificador, la dirección IP y el país al que pertenece y se presentan las opciones de buscar, adicionar, modificar y eliminar.
• buscar dirección IP: para ello, se teclea la dirección IP que se quiere buscar y como resultado se muestra el identificador, la dirección IP seleccionada y el país al que pertenece, en caso de no encontrarse la dirección IP se muestra que: “La dirección IP no fue encontrada”
• adicionar dirección IP: para ello se introduce la dirección IP y el país de donde procede la petición sospechosa, al adicionarse se muestra el mensaje: La Dirección IP “dirección IP” fue agregada correctamente, en caso de no entrar un valor válido para la dirección IP se muestra el siguiente mensaje: Introduzca una dirección IPv4 o IPv6 válida, en caso de entrar una dirección IP que ya existe para el país especificado se muestra el mensaje que ya existe esa dirección IP para el país especificado.
• modificar dirección IP: para ello se busca la dirección IP que se quiere modificar y se cliquea sobre la misma, al modificar se muestra el mensaje: La dirección IP “dirección” se cambió correctamente.
• eliminar dirección IP: para ello se selecciona la dirección IP que se quiere eliminar, antes de eliminarla se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar la dirección IP seleccionada? Todos los siguientes objetos y sus elementos relacionados serán borrados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 Dirección IP satisfactoriamente.
• Filtrar: se tiene la posibilidad de filtrar las direcciones IP por países, para ello en el filtro se selecciona el nombre del país que se quiera filtrar y se muestra el identificador y la dirección IP asociadas al país seleccionado.</td></tr>
<tr><td colspan="3">Prototipo elemental de interfaz gráfica de usuario:
 
</td></tr>
</table>

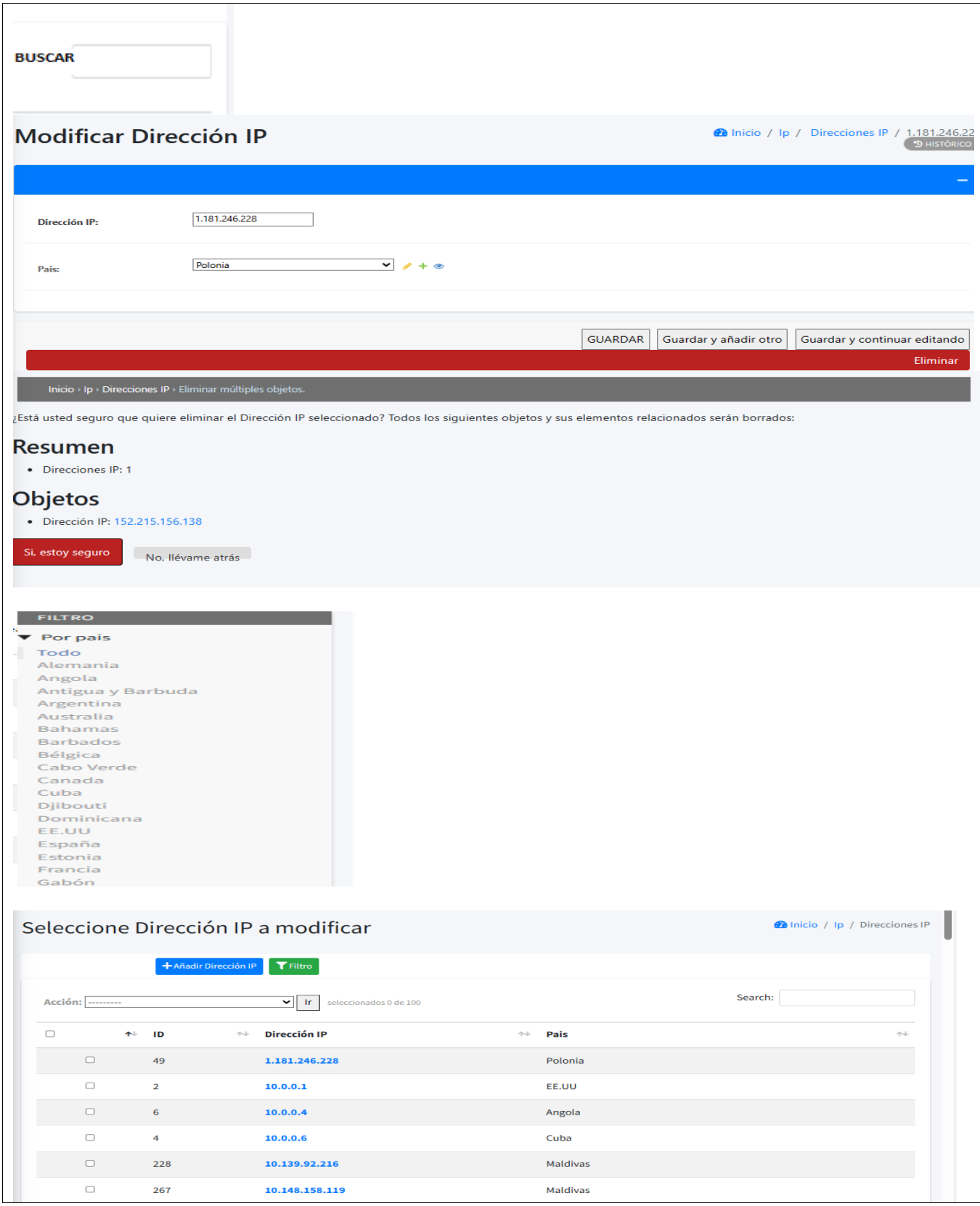
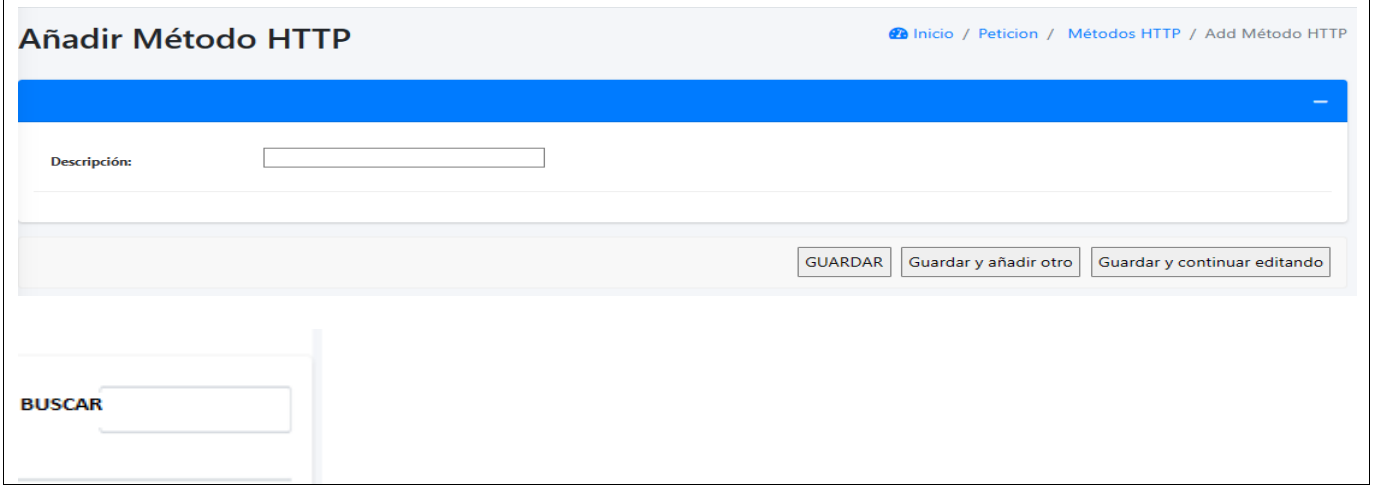

BUSCAR
Modificar Dirección IP
Inicio / Ip / Direcciones IP / 1.181.246.22
HISTÓRICO
Dirección IP:
1.181.246.228
Pais:
Polonia
GUARDAR
Guardar y añadir otro
Guardar y continuar editando
Eliminar
Inicio › Ip › Direcciones IP › Eliminar múltiples objetos.
¿Está usted seguro que quiere eliminar el Dirección IP seleccionado? Todos los siguientes objetos y sus elementos relacionados serán borrados:
Resumen
Direcciones IP: 1
Objetos
Dirección IP: 152.215.156.138
Si, estoy seguro
No, llévame atrás
FILTRO
Por pais
Todo
Alemania
Angola
Antigua y Barbuda
Argentina
Australia
Bahamas
Barbados
Bélgica
Cabo Verde
Canada
Cuba
Djibouti
Dominicana
EE.UU
España
Estonia
Francia
Gabón
Seleccione Dirección IP a modificar
Inicio / Ip / Direcciones IP
Añadir Dirección IP
Filtro
Acción:
Ir
seleccionados 0 de 100
Search:
ID
Dirección IP
Pais
49
1.181.246.228
Polonia
2
10.0.0.1
EE.UU
6
10.0.0.4
Angola
4
10.0.0.6
Cuba
228
10.139.92.216
Maldivas
267
10.148.158.119
Maldivas

Tabla 41 Historia de Usuario #3

<table>
<tr><td colspan="2">Historia de Usuario</td></tr>
<tr><td>Número: HU_3</td><td>Requisito: Gestionar Método HTTP</td></tr>
<tr><td colspan="2">Usuario: Administrador</td></tr>
<tr><td>Prioridad en el negocio: Alta</td><td>Riesgo en Desarrollo: Medio</td></tr>
<tr><td>Puntos estimados: 0.3</td><td>Iteración Asignada: 1</td></tr>
<tr><td colspan="2">Programador responsable: Yadira Sánchez Cruz</td></tr>
<tr><td colspan="2">Descripción: El administrador requiere gestionar los datos de los métodos HTTP utilizados para realizar las peticiones sospechosas, para lo cual se muestra una lista de los mismos con su identificador y su descripción y se presentan las opciones de buscar, adicionar, modificar y eliminar.
• buscar método HTTP: para ello, se teclea la descripción del método HTTP que se quiere buscar y como resultado se muestra el identificador y la descripción del método HTTP seleccionado, en caso de no encontrarse el método HTTP se muestra que: “El método HTTP no fue encontrado”
• adicionar método HTTP: para ello se introduce la descripción del método HTTP que usaron en la petición sospechosa, al adicionarse se muestra el mensaje: El método HTTP “descripción del método” fue agregado correctamente, en caso de que exista el método HTTP se muestra que ya existe un Método HTTP con esa descripción
• modificar método HTTP: para ello se busca la descripción del método que se quiere modificar y se cliquea sobre la misma, al modificar se muestra el mensaje: El método HTTP “descripción del método HTTP” se cambió correctamente.
• eliminar método HTTP: para ello se selecciona el método HTTP que se quiere eliminar, antes de eliminarlo se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar el Método HTTP seleccionado? Todos los siguientes objetos y sus elementos relacionados serán eliminados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 Método HTTP satisfactoriamente.</td></tr>
<tr><td colspan="2">Prototipo elemental de interfaz gráfica de usuario:
 
</td></tr>
</table>

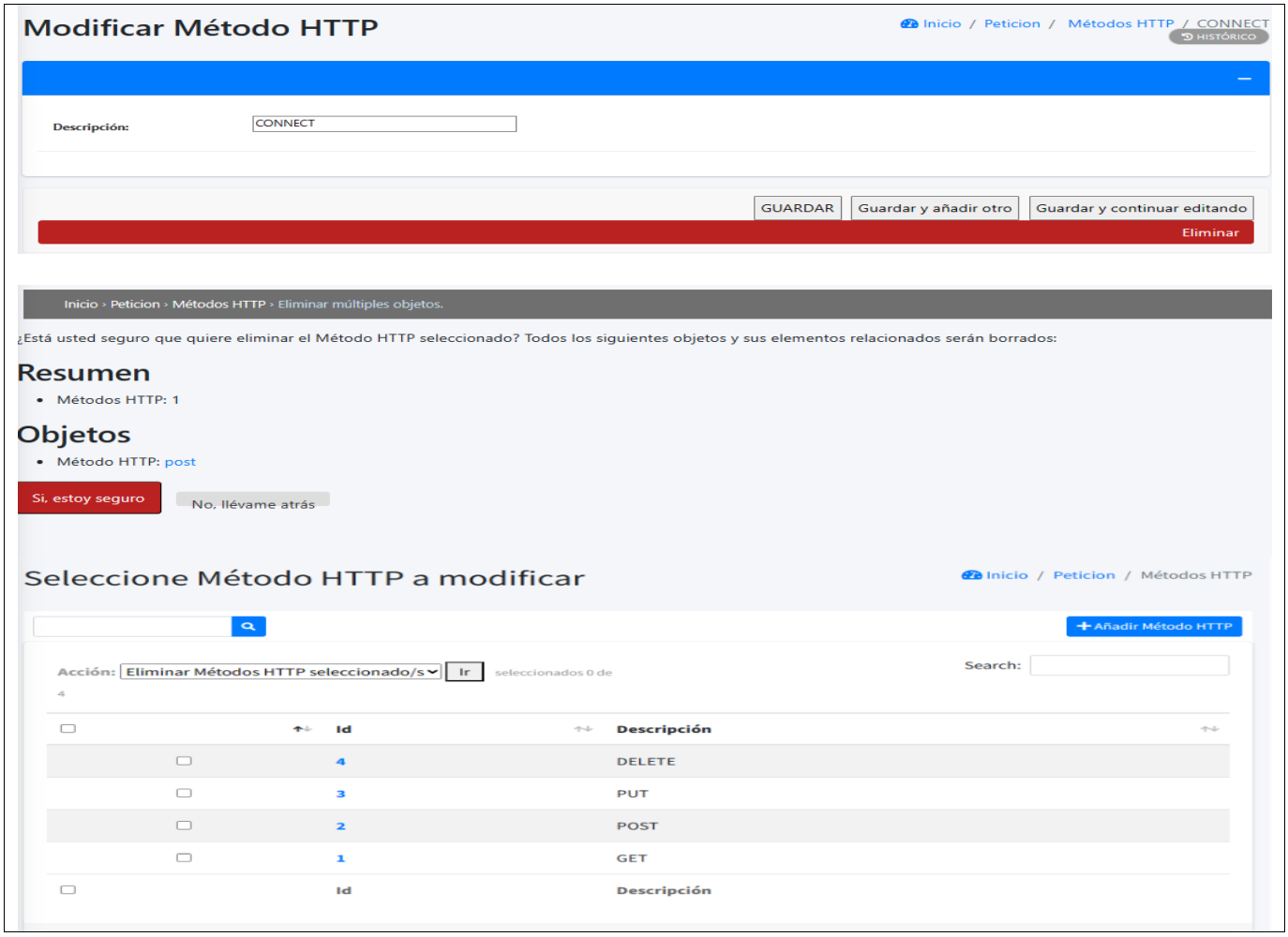


Tabla 42 Historia de Usuario #4

Historia de Usuario	
Número: HU_4	**Requisito:** Gestionar Código de Respuesta HTTP
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 0.3	**Iteración Asignada:** 1
Programador responsable: Yadira Sánchez Cruz	
Descripción: El administrador requiere gestionar los datos de los códigos de respuestas HTTP proporcionados, para lo cual se muestra una lista de los mismos con su identificador y su descripción y se presentan las opciones de buscar, adicionar, modificar y eliminar. • **buscar código de respuesta HTTP**: para ello, se teclea la descripción del código de respuesta HTTP que se quiere buscar y como resultado se muestra el identificador y la descripción del código de respuesta HTTP seleccionado, en caso de no encontrarse el código de respuesta HTTP se muestra que: “El código de respuesta HTTP no fue encontrado” • **adicionar código de respuesta HTTP**: para ello se introduce la descripción del código de respuesta HTTP, al adicionarse se muestra el mensaje: El código de respuesta HTTP “descripción del código de respuesta” fue agregado correctamente, en caso de que exista el código de respuesta se muestra que ya existe un código de respuesta HTTP con esa	

descripción

- **modificar código de respuesta HTTP**: para ello se busca la descripción del código de respuesta que se quiere modificar y se cliquea sobre el mismo, al modificar se muestra el mensaje: El código de respuesta HTTP “descripción del código de respuesta HTTP” se cambió correctamente.
- **eliminar código de respuesta HTTP**: para ello se selecciona el código de respuesta HTTP que se quiere eliminar, antes de eliminarlo se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar el código de respuesta HTTP seleccionado? Todos los siguientes objetos y sus elementos relacionados serán eliminados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 Código de respuesta HTTP satisfactoriamente.

Prototipo elemental de interfaz gráfica de usuario:

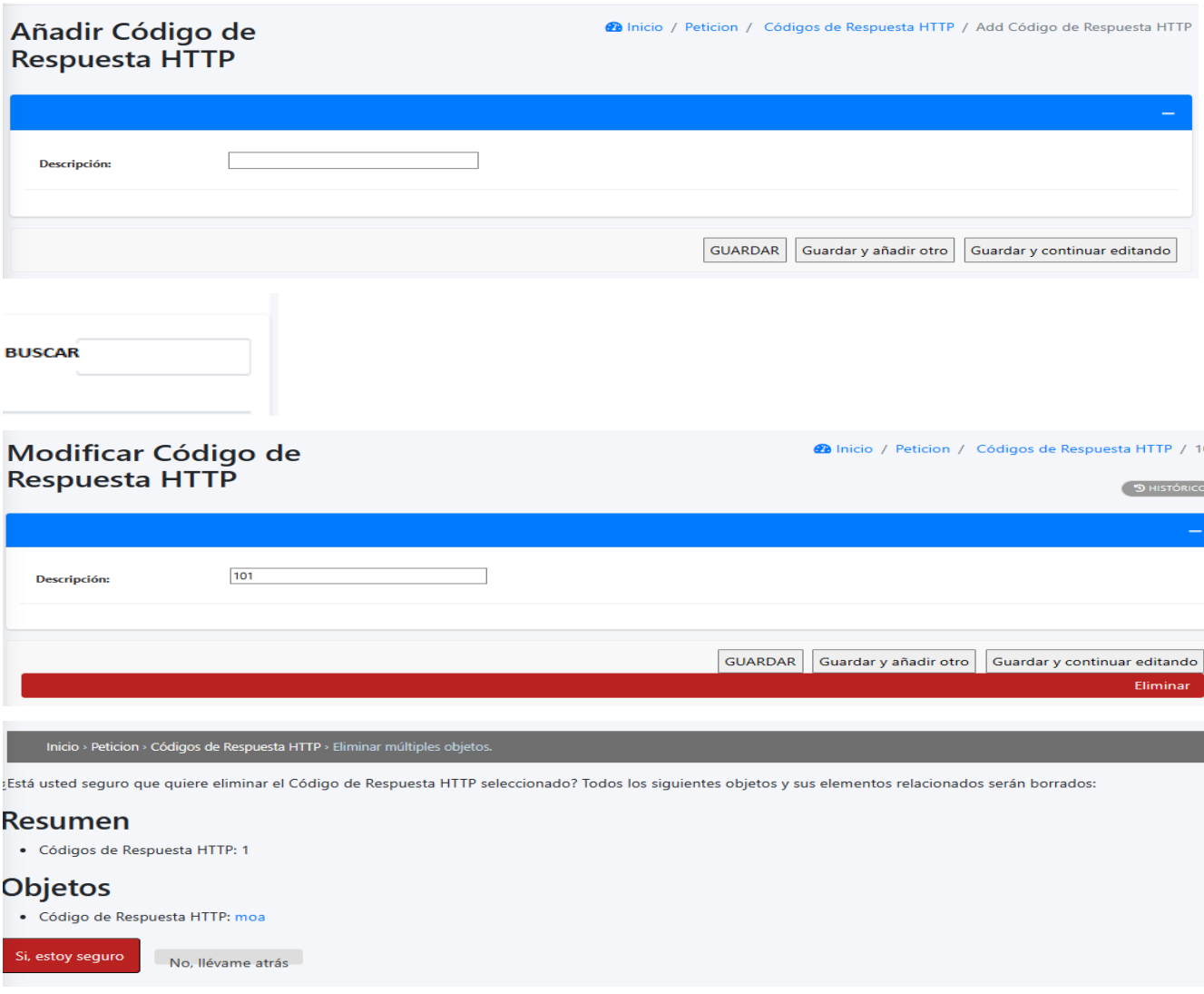


Tabla 43 Historia de Usuario #5

Historia de Usuario	
Número: HU_5	**Requisito:** Gestionar Agente de Usuario
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 0.3	**Iteración Asignada:** 1
Programador responsable: Yadira Sánchez Cruz	
Descripción: El administrador requiere gestionar los datos de los agentes de usuarios utilizados para la realizar la petición sospechosa, para lo cual se muestra una lista de los mismos con su identificador y su descripción y se presentan las opciones de buscar, adicionar, modificar y eliminar. • **buscar agente de usuario**: para ello, se teclea la descripción del agente de usuario que se quiere buscar y como resultado se muestra el identificador y la descripción del agente de usuario seleccionado, en caso de no encontrarse el agente de usuario se muestra que: "El agente de usuario no fue encontrado" • **adicionar agente de usuario**: para ello se introduce la descripción del agente de usuario, al adicionarse se muestra el mensaje: El agente de usuario "descripción del agente de usuario" fue agregado correctamente, en caso de que exista el agente de usuario se muestra que ya existe un agente de usuario con esa descripción • **modificar agente de usuario**: para ello se busca la descripción del agente de usuario que se quiere modificar y se cliquea sobre el mismo, al modificar se muestra el mensaje: El agente de usuario "descripción del agente de usuario" se cambió correctamente. • **eliminar agente de usuario**: para ello se selecciona el agente de usuario que se quiere eliminar, antes de eliminarlo se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar el agente de usuario seleccionado? Todos los siguientes objetos y sus elementos relacionados serán eliminados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 Agente de Usuario satisfactoriamente.	
Prototipo elemental de interfaz gráfica de usuario:	

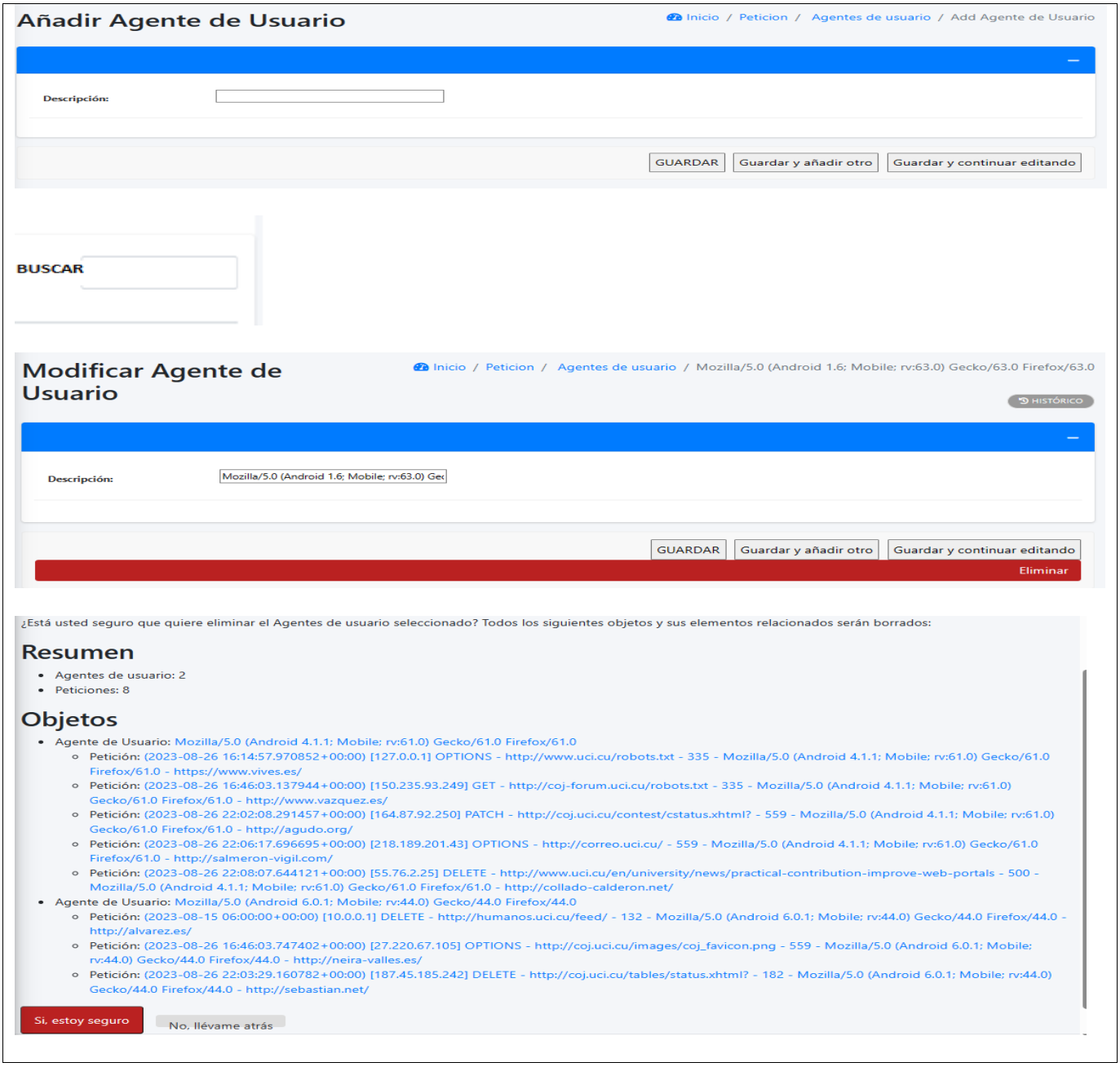

Añadir Agente de Usuario
Inicio / Peticion / Agentes de usuario / Add Agente de Usuario
Descripción:
GUARDAR
Guardar y añadir otro
Guardar y continuar editando
BUSCAR
Modificar Agente de Usuario
Inicio / Peticion / Agentes de usuario / Mozilla/5.0 (Android 1.6; Mobile; rv:63.0) Gecko/63.0 Firefox/63.0
HISTÓRICO
Descripción:
Mozilla/5.0 (Android 1.6; Mobile; rv:63.0) Gec
GUARDAR
Guardar y añadir otro
Guardar y continuar editando
Eliminar
¿Está usted seguro que quiere eliminar el Agentes de usuario seleccionado? Todos los siguientes objetos y sus elementos relacionados serán borrados:
Resumen
Agentes de usuario: 2
Peticiones: 8
Objetos
Agente de Usuario: Mozilla/5.0 (Android 4.1.1; Mobile; rv:61.0) Gecko/61.0 Firefox/61.0
Petición: (2023-08-26 16:14:57.970852+00:00) [127.0.0.1] OPTIONS - http://www.uci.cu/robots.txt - 335 - Mozilla/5.0 (Android 4.1.1; Mobile; rv:61.0) Gecko/61.0 Firefox/61.0 - https://www.vives.es/
Petición: (2023-08-26 16:46:03.137944+00:00) [150.235.93.249] GET - http://coj-forum.uci.cu/robots.txt - 335 - Mozilla/5.0 (Android 4.1.1; Mobile; rv:61.0) Gecko/61.0 Firefox/61.0 - http://www.vazquez.es/
Petición: (2023-08-26 22:02:08.291457+00:00) [164.87.92.250] PATCH - http://coj.uci.cu/contest/cstatus.xhtml? - 559 - Mozilla/5.0 (Android 4.1.1; Mobile; rv:61.0) Gecko/61.0 Firefox/61.0 - http://agudo.org/
Petición: (2023-08-26 22:06:17.696695+00:00) [218.189.201.43] OPTIONS - http://correo.uci.cu/ - 559 - Mozilla/5.0 (Android 4.1.1; Mobile; rv:61.0) Gecko/61.0 Firefox/61.0 - http://salmeron-vigil.com/
Petición: (2023-08-26 22:08:07.644121+00:00) [55.76.2.25] DELETE - http://www.uci.cu/en/university/news/practical-contribution-improve-web-portals - 500 - Mozilla/5.0 (Android 4.1.1; Mobile; rv:61.0) Gecko/61.0 Firefox/61.0 - http://collado-calderon.net/
Agente de Usuario: Mozilla/5.0 (Android 6.0.1; Mobile; rv:44.0) Gecko/44.0 Firefox/44.0
Petición: (2023-08-15 06:00:00+00:00) [10.0.0.1] DELETE - http://humanos.uci.cu/feed/ - 132 - Mozilla/5.0 (Android 6.0.1; Mobile; rv:44.0) Gecko/44.0 Firefox/44.0 - http://alvarez.es/
Petición: (2023-08-26 16:46:03.747402+00:00) [27.220.67.105] OPTIONS - http://coj.uci.cu/images/coj_favicon.png - 559 - Mozilla/5.0 (Android 6.0.1; Mobile; rv:44.0) Gecko/44.0 Firefox/44.0 - http://neira-valles.es/
Petición: (2023-08-26 22:03:29.160782+00:00) [187.45.185.242] DELETE - http://coj.uci.cu/tables/status.xhtml? - 182 - Mozilla/5.0 (Android 6.0.1; Mobile; rv:44.0) Gecko/44.0 Firefox/44.0 - http://sebastian.net/
Si, estoy seguro
No, llévame atrás

Tabla 44 Historia de Usuario #6

Historia de Usuario	
Número: HU_6	**Requisito:** Gestionar Referencia
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 0.3	**Iteración Asignada:** 1
Programador responsable: Yadira Sánchez Cruz	
Descripción: El administrador requiere gestionar los datos de la referencia utilizada para realizar la petición sospechosa, para lo cual se muestra una lista de los mismos con su identificador y su descripción y se presentan las opciones de buscar, adicionar, modificar y eliminar. • **buscar referencia**: para ello, se teclea la descripción de la referencia que se quiere buscar y como resultado se muestra el identificador y la descripción de la referencia seleccionada, en caso de no encontrarse la referencia se muestra que: “La referencia no fue encontrada” • **adicionar referencia**: para ello se introduce la descripción de la referencia, al adicionarse se muestra el mensaje: La referencia “descripción de la referencia” fue agregada correctamente, en caso de que exista la referencia se muestra que ya existe una referencia con esa descripción • **modificar referencia**: para ello se busca la descripción de la referencia que se quiere modificar y se cliquea sobre la misma, al modificar se muestra el mensaje: La referencia “descripción de la referencia” se cambió correctamente. • **eliminar referencia**: para ello se selecciona la referencia que se quiere eliminar, antes de eliminarla se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar la referencia seleccionada? Todos los siguientes objetos y sus elementos relacionados serán eliminados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 Referencia satisfactoriamente.	
Prototipo elemental de interfaz gráfica de usuario:	

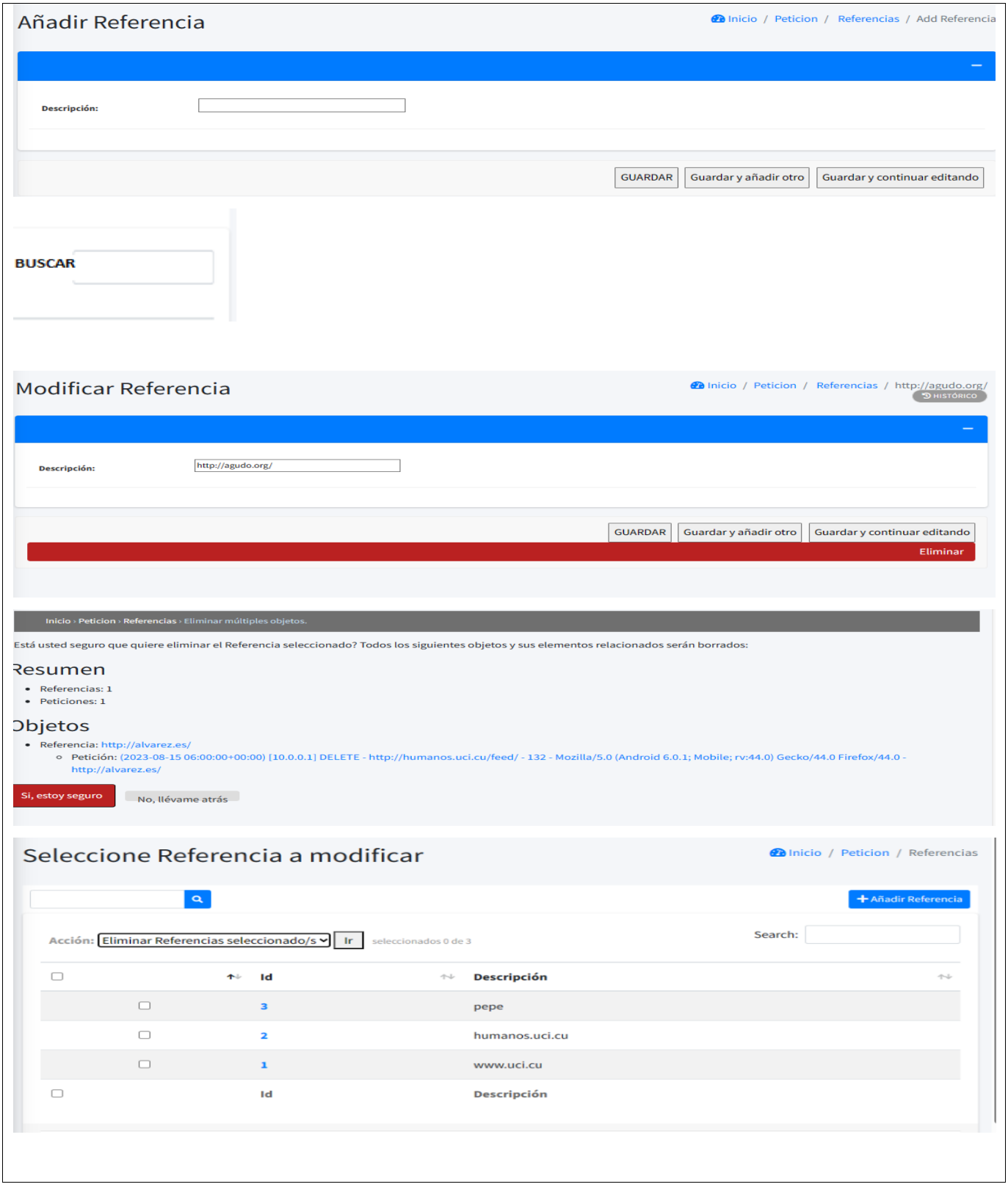
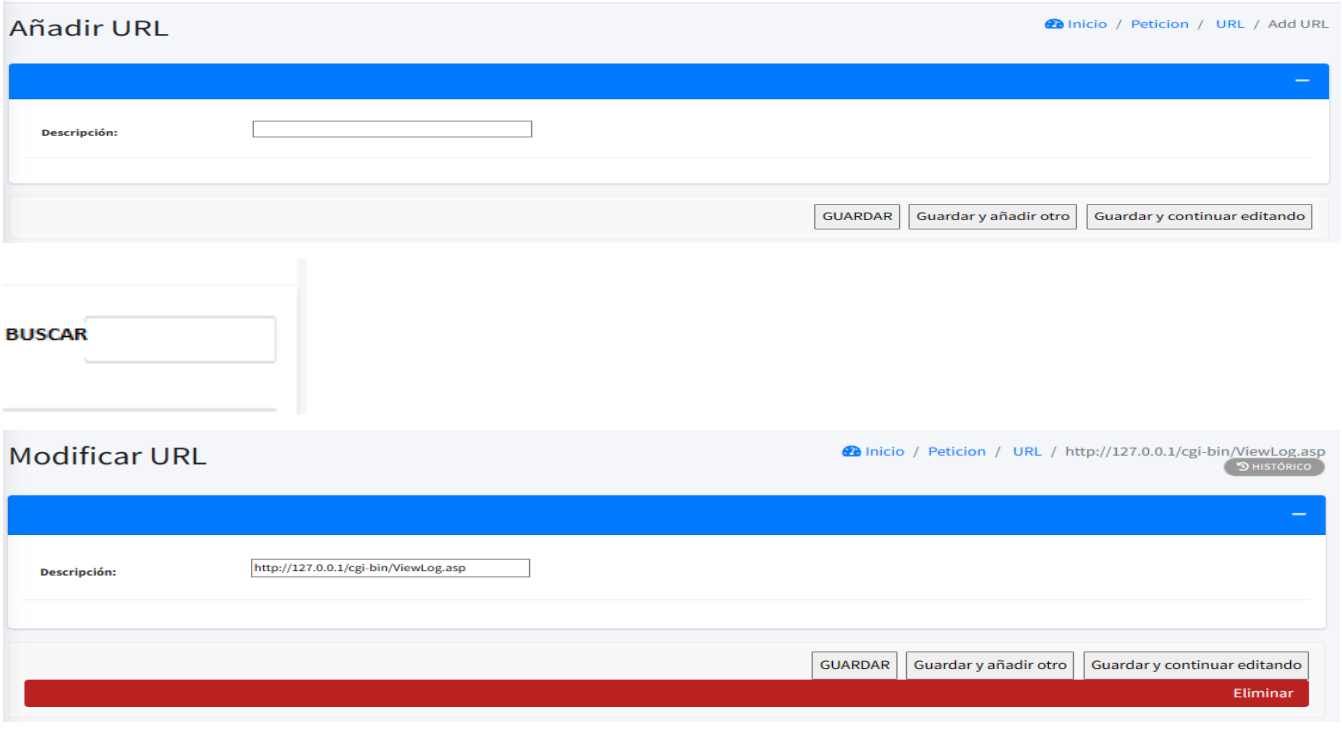

Añadir Referencia
Inicio / Peticion / Referencias / Add Referencia
Descripción:
GUARDAR
Guardar y añadir otro
Guardar y continuar editando
BUSCAR
Modificar Referencia
Inicio / Peticion / Referencias / http://agudo.org/
HISTÓRICO
Descripción:
http://agudo.org/
GUARDAR
Guardar y añadir otro
Guardar y continuar editando
Eliminar
Inicio › Peticion › Referencias › Eliminar múltiples objetos.
Está usted seguro que quiere eliminar el Referencia seleccionado? Todos los siguientes objetos y sus elementos relacionados serán borrados:
Resumen
Referencias: 1
Peticiones: 1
Objetos
Referencia: http://alvarez.es/
Petición: (2023-08-15 06:00:00+00:00) [10.0.0.1] DELETE - http://humanos.uci.cu/feed/ - 132 - Mozilla/5.0 (Android 6.0.1; Mobile; rv:44.0) Gecko/44.0 Firefox/44.0 - http://alvarez.es/
Si, estoy seguro
No, llévame atrás
Seleccione Referencia a modificar
Inicio / Peticion / Referencias
Añadir Referencia
Acción: Eliminar Referencias seleccionado/s
Ir
seleccionados 0 de 3
Search:
Id
Descripción
3
pepe
2
humanos.uci.cu
1
www.uci.cu
Id
Descripción

Tabla 45 Historia de Usuario #7

<table>
<tr><td colspan="3">Historia de Usuario</td></tr>
<tr><td>Número: HU_7</td><td colspan="2">Requisito: Gestionar URL</td></tr>
<tr><td colspan="3">Usuario: Administrador</td></tr>
<tr><td colspan="2">Prioridad en el negocio: Alta</td><td>Riesgo en Desarrollo: Medio</td></tr>
<tr><td colspan="2">Puntos estimados: 0.3</td><td>Iteración Asignada: 1</td></tr>
<tr><td colspan="3">Programador responsable: Yadira Sánchez Cruz</td></tr>
<tr><td colspan="3">Descripción: El administrador requiere gestionar los datos de la URL utilizada para realizar la petición sospechosa, para lo cual se muestra una lista de los mismos con su identificador y su descripción y se presentan las opciones de buscar, adicionar, modificar y eliminar.
• buscar URL: para ello, se teclea la descripción de la URL que se quiere buscar y como resultado se muestra el identificador y la descripción de la URL seleccionada, en caso de no encontrarse la URL se muestra que: “La URL no fue encontrada”
• adicionar URL: para ello se introduce la descripción de la URL, al adicionarse se muestra el mensaje: La URL “descripción de la URL” fue agregada correctamente, en caso de que exista la URL se muestra que ya existe una URL con esa descripción
• modificar URL: para ello se busca la descripción de la URL que se quiere modificar y se cliquea sobre la misma, al modificar se muestra el mensaje: La URL “descripción de la URL” se cambió correctamente.
• eliminar URL: para ello se selecciona la URL que se quiere eliminar, antes de eliminarla se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar la URL seleccionada? Todos los siguientes objetos y sus elementos relacionados serán eliminados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 URL satisfactoriamente.</td></tr>
<tr><td colspan="3">Prototipo elemental de interfaz gráfica de usuario:
 
</td></tr>
</table>

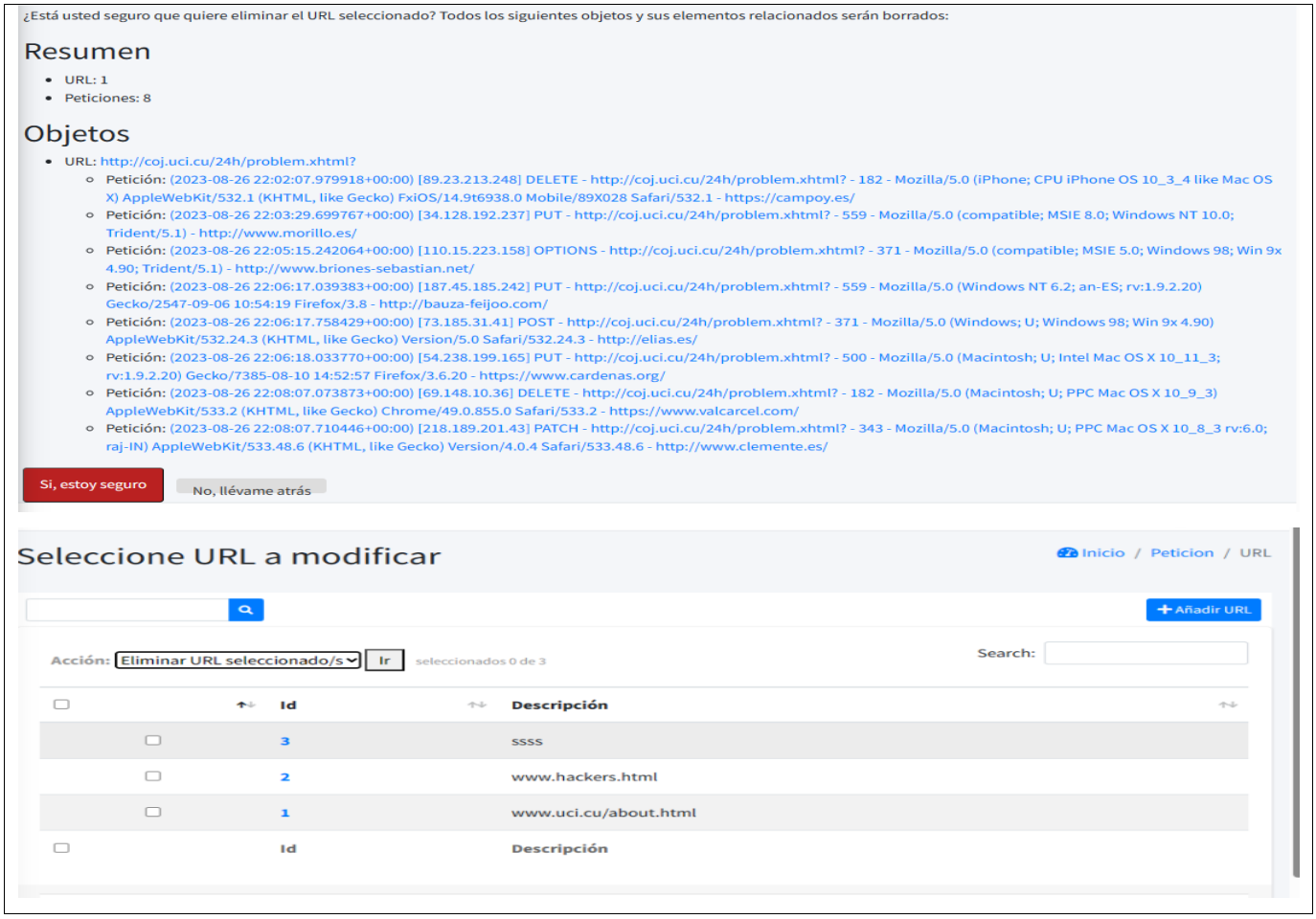


Tabla 46 Historia de Usuario #8

Historia de Usuario	
Número: HU_8	**Requisito:** Gestionar Tecnología
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 0.3	**Iteración Asignada:** 1
Programador responsable: Yadira Sánchez Cruz	
Descripción: El administrador requiere gestionar los datos de la tecnología atacada por la petición sospechosa, para lo cual se muestra una lista de los mismos con su identificador y su descripción y se presentan las opciones de buscar, adicionar, modificar y eliminar. • **buscar tecnología**: para ello, se teclea la descripción de la tecnología que se quiere buscar y como resultado se muestra el identificador y la descripción de la tecnología seleccionada, en caso de no encontrarse la tecnología se muestra que: “La tecnología no fue encontrada” • **adicionar tecnología**: para ello se introduce la descripción de la tecnología, al adicionarse se muestra el mensaje: La tecnología “descripción de la tecnología” fue agregada correctamente, en caso de que exista la tecnología se muestra que ya existe una tecnología con esa descripción • **modificar tecnología**: para ello se busca la descripción de la tecnología que se quiere modificar y se cliquea sobre la misma, al modificar se muestra el mensaje: La tecnología	

"descripción de la tecnología" se cambió correctamente.

- **eliminar tecnología**: para ello se selecciona la tecnología que se quiere eliminar, antes de eliminarla se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar la tecnología seleccionada? Todos los siguientes objetos y sus elementos relacionados serán eliminados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 Tecnología satisfactoriamente.

Prototipo elemental de interfaz gráfica de usuario:

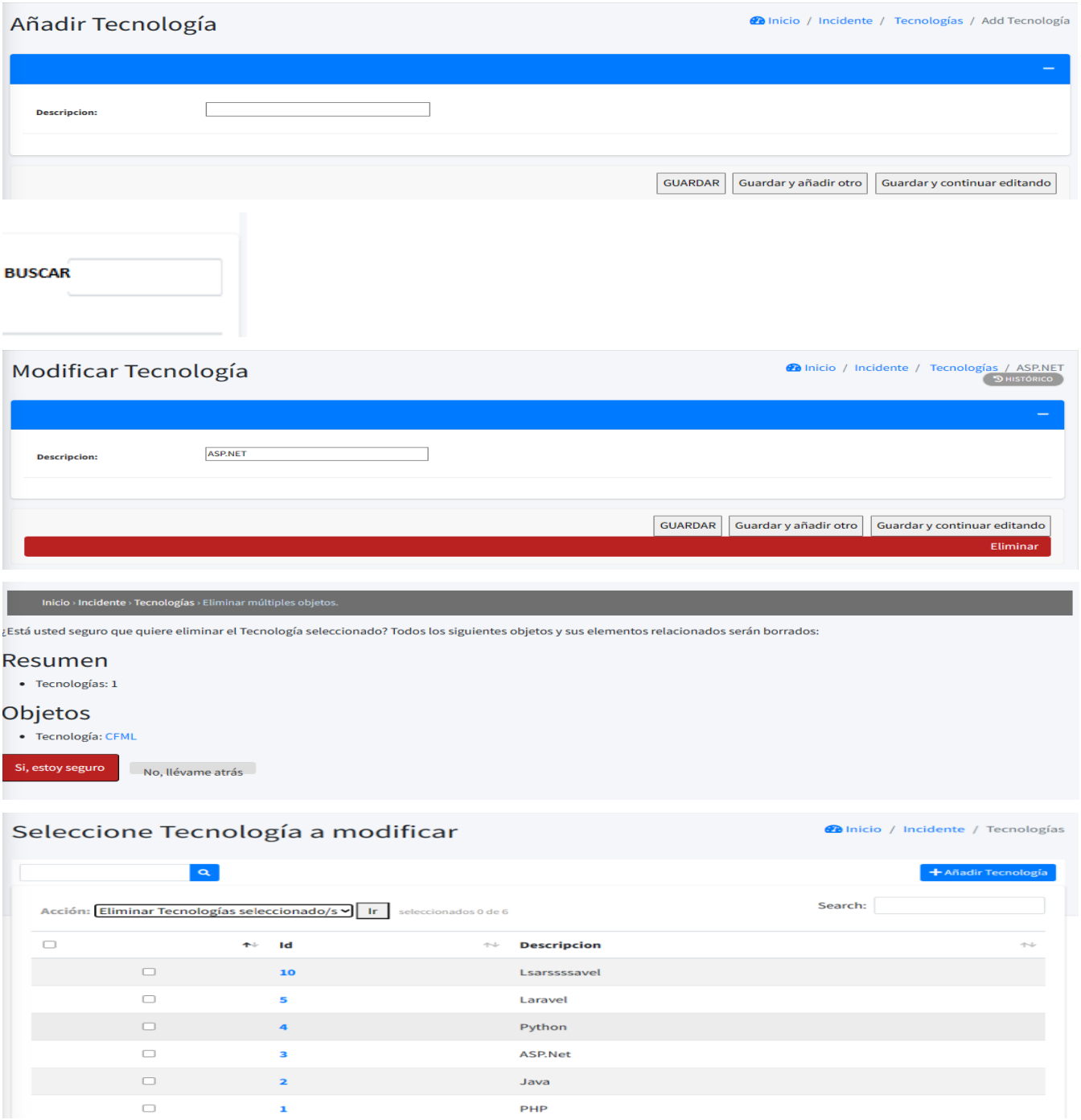
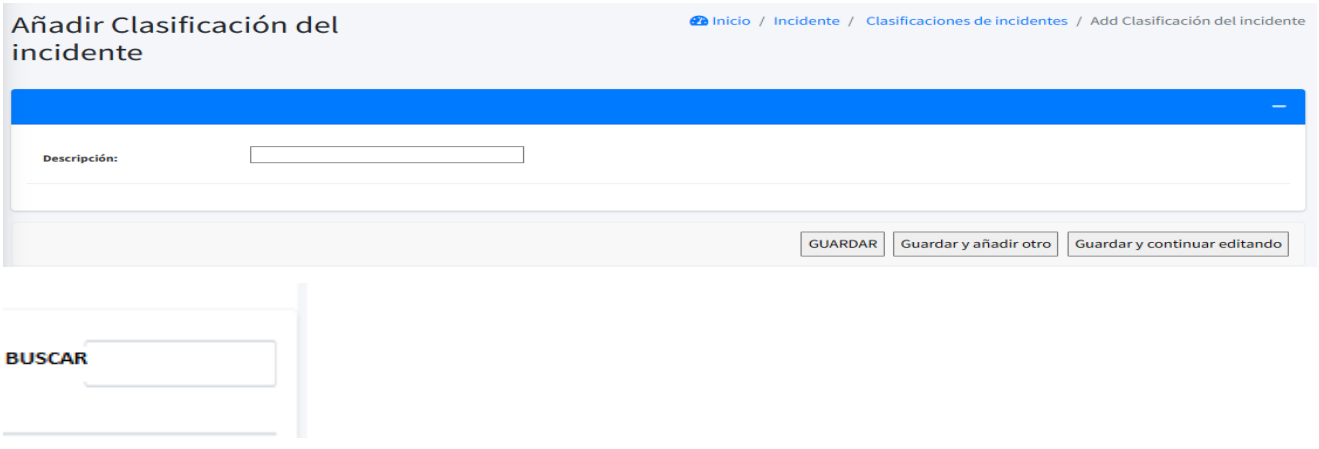


Tabla 47 Historia de Usuario #9

<table>
<tr><td colspan="2">Historia de Usuario</td></tr>
<tr><td>Número: HU_9</td><td>Requisito: Gestionar Clasificación del Incidente</td></tr>
<tr><td colspan="2">Usuario: Administrador</td></tr>
<tr><td>Prioridad en el negocio: Alta</td><td>Riesgo en Desarrollo: Medio</td></tr>
<tr><td>Puntos estimados: 0.3</td><td>Iteración Asignada: 1</td></tr>
<tr><td colspan="2">Programador responsable: Yadira Sánchez Cruz</td></tr>
<tr><td colspan="2">Descripción: El administrador requiere gestionar los datos de la clasificación del incidente, para lo cual se muestra una lista de los mismos con su identificador y su descripción y se presentan las opciones de buscar, adicionar, modificar y eliminar.
• buscar clasificación del incidente: para ello, se teclea la descripción de la clasificación del incidente que se quiere buscar y como resultado se muestra el identificador y la descripción de la clasificación seleccionada, en caso de no encontrarse la clasificación del incidente se muestra que: “La clasificación del incidente no fue encontrada”
• adicionar clasificación del incidente: para ello se introduce la descripción de la clasificación del incidente, al adicionarse se muestra el mensaje: La clasificación del incidente “descripción de la clasificación del incidente” fue agregada correctamente, en caso de que exista la clasificación se muestra que ya existe una clasificación de incidente con esa descripción
• modificar clasificación del incidente: para ello se busca la descripción de la clasificación del incidente que se quiere modificar y se cliquea sobre la misma, al modificar se muestra el mensaje: La clasificación del incidente “descripción de la clasificación del incidente” se cambió correctamente.
• eliminar clasificación del incidente: para ello se selecciona la clasificación del incidente que se quiere eliminar, antes de eliminarla se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar la clasificación del incidente seleccionada? Todos los siguientes objetos y sus elementos relacionados serán eliminados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 Clasificación del incidente satisfactoriamente</td></tr>
<tr><td colspan="2">Prototipo elemental de interfaz gráfica de usuario:
 
</td></tr>
</table>

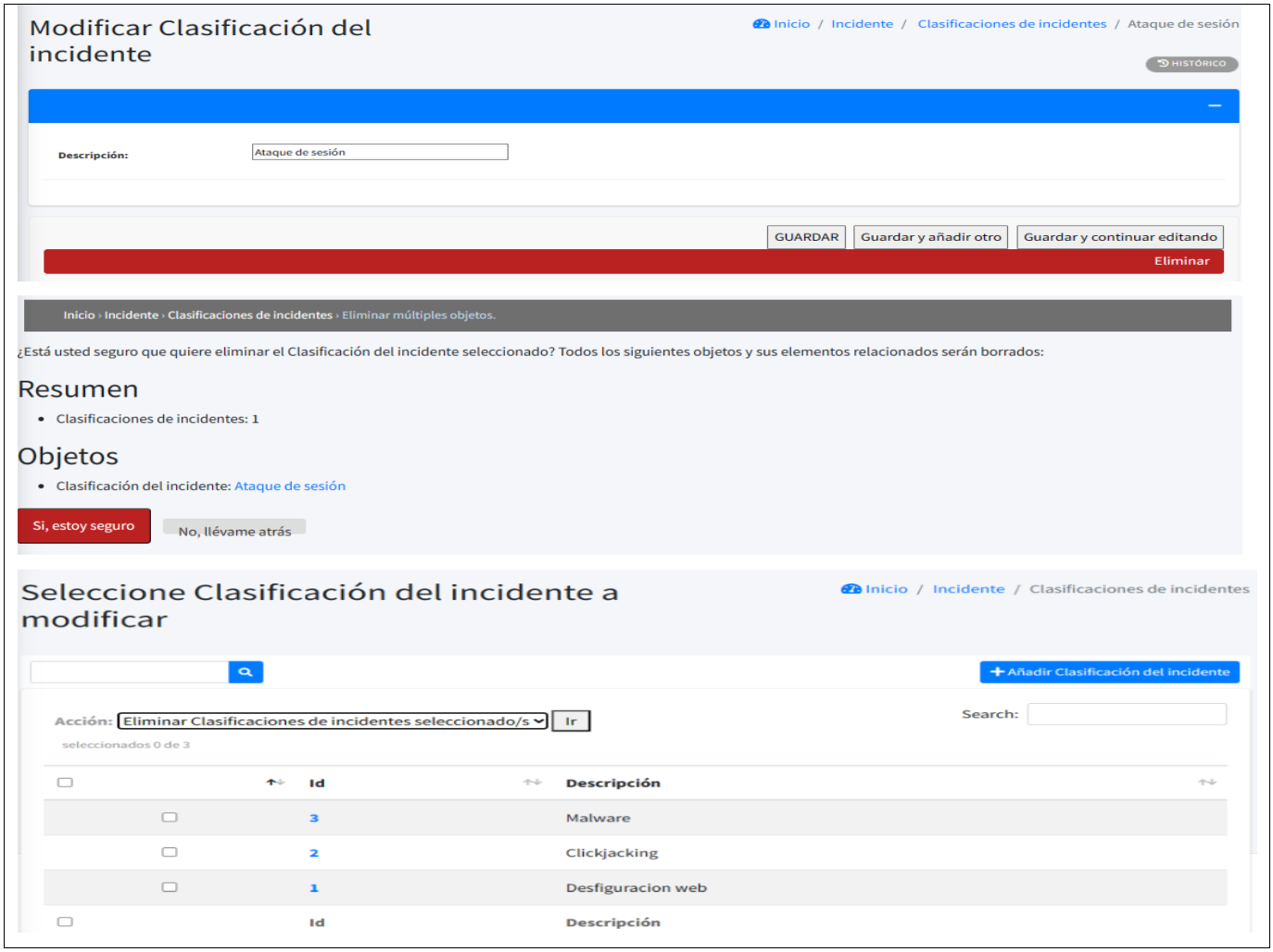


Tabla 48 Historia de Usuario #10

Historia de Usuario	
Número: HU_10	**Requisito:** Gestionar Entidades
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 0.3	**Iteración Asignada:** 1
Programador responsable: Yadira Sánchez Cruz	
Descripción: El administrador requiere gestionar los datos de la entidad a la que se envió la petición sospechosa, para lo cual se muestra una lista de los mismos con su identificador y su nombre y se presentan las opciones de buscar, adicionar, modificar y eliminar. • **buscar entidad**: para ello, se teclea el nombre de la entidad que se quiere buscar y como resultado se muestra el identificador y el nombre de la entidad, en caso de no encontrarse la entidad se muestra que: “La entidad no fue encontrada” • **adicionar entidad**: para ello se introduce el nombre de la entidad, al adicionarse se muestra el mensaje: La entidad “nombre de la entidad” fue agregada correctamente, en caso de que exista la entidad se muestra que ya existe la entidad. • **modificar entidad**: para ello se busca de la entidad que se quiere modificar y se cliquea sobre	

el mismo, al modificar se muestra el mensaje: La entidad “nombre de la entidad” se cambió correctamente.

- **eliminar entidad**: para ello se selecciona la entidad que se quiere eliminar, antes de eliminarla se muestra el siguiente mensaje: ¿Está usted seguro que quiere eliminar la entidad seleccionada? Todos los siguientes objetos y sus elementos relacionados serán eliminados, en caso de aceptar el sistema muestra el siguiente mensaje: Eliminado/s 1 Entidad satisfactoriamente

Prototipo elemental de interfaz gráfica de usuario:

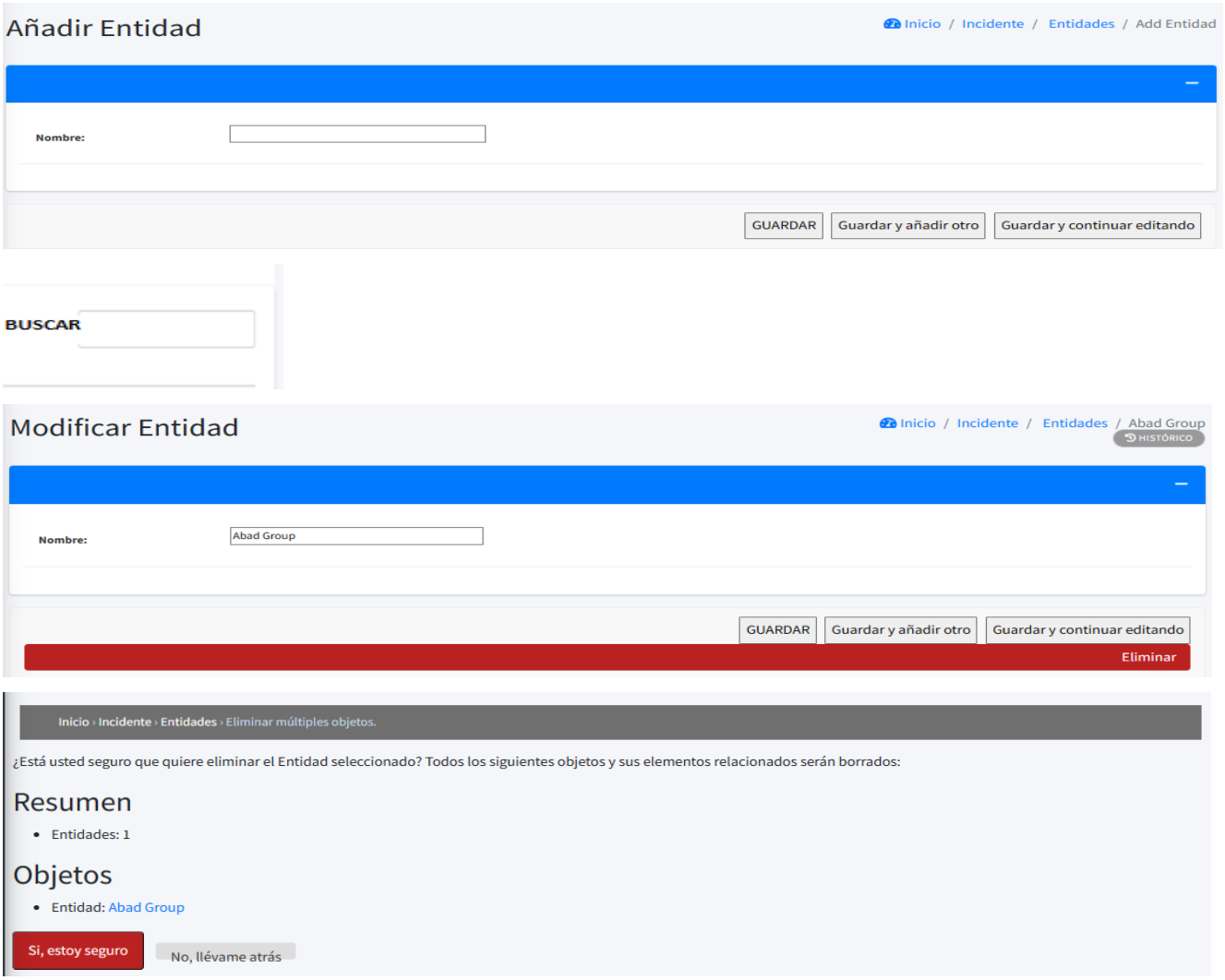
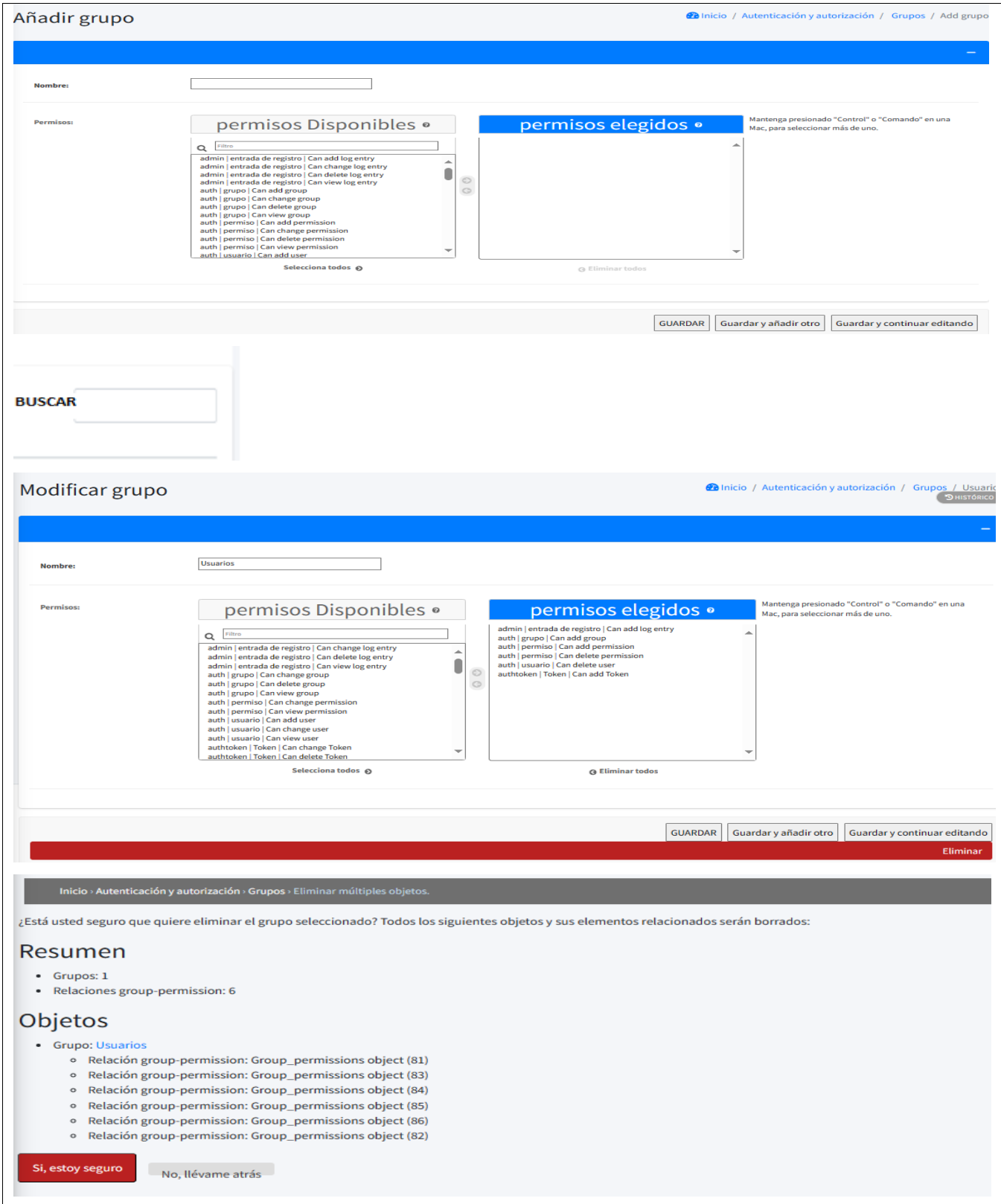


Tabla 49 Historia de Usuario #13

Historia de Usuario	
Número: HU_13	**Requisito:** Gestionar Grupo
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 0.3	**Iteración Asignada:** 2
Programador responsable: Yadira Sánchez Cruz	
Descripción: El administrador requiere gestionar los datos referentes los grupos y roles que tendrá el sistema y se presentan las opciones de buscar, adicionar, modificar y eliminar. • **buscar grupo**: para ello, se teclea el nombre del grupo que se quiere buscar y como resultado se muestra el identificador y el nombre del grupo, en caso de no encontrarse el grupo se muestra que: "El grupo no fue encontrado" • **adicionar grupo**: para ello se introduce el nombre del grupo, y se seleccionan los permisos que tendrá asociado el grupo, al adicionarse se muestra un mensaje: El grupo "nombre del grupo" fue agregado correctamente. en caso de que exista el grupo se muestra que ya existe el grupo con los permisos especificados. • **modificar grupo**: para ello se busca el grupo que se quiere modificar y se cliquea sobre el mismo, al modificarse se muestra el mensaje: El Grupo "nombre del grupo" se cambió correctamente. • **eliminar grupo**: para ello se selecciona el grupo que se quiere eliminar, antes de eliminarlo se emite el siguiente mensaje: ¿Está usted seguro que quiere eliminar el grupo seleccionado? Todos los siguientes objetos y sus elementos relacionados serán borrados, en caso de aceptar el sistema especifica lo siguiente: Eliminado/s 1 Grupo satisfactoriamente	
Prototipo elemental de interfaz gráfica de usuario:	


Añadir grupo
Inicio / Autenticación y autorización / Grupos / Add grupo
Nombre:
Permisos:
permisos Disponibles
permisos elegidos
Mantenga presionado "Control" o "Comando" en una Mac, para seleccionar más de uno.
admin | entrada de registro | Can add log entry
admin | entrada de registro | Can change log entry
admin | entrada de registro | Can delete log entry
admin | entrada de registro | Can view log entry
auth | grupo | Can add group
auth | grupo | Can change group
auth | grupo | Can delete group
auth | grupo | Can view group
auth | permiso | Can add permission
auth | permiso | Can change permission
auth | permiso | Can delete permission
auth | permiso | Can view permission
auth | usuario | Can add user
Selecciona todos
Eliminar todos
GUARDAR
Guardar y añadir otro
Guardar y continuar editando
BUSCAR
Modificar grupo
Inicio / Autenticación y autorización / Grupos / Usuario
HISTÓRICO
Nombre:
Usuarios
Permisos:
permisos Disponibles
permisos elegidos
Mantenga presionado "Control" o "Comando" en una Mac, para seleccionar más de uno.
admin | entrada de registro | Can add log entry
auth | grupo | Can add group
auth | permiso | Can add permission
auth | permiso | Can delete permission
auth | usuario | Can delete user
authtoken | Token | Can add Token
admin | entrada de registro | Can change log entry
admin | entrada de registro | Can delete log entry
admin | entrada de registro | Can view log entry
auth | grupo | Can change group
auth | grupo | Can delete group
auth | grupo | Can view group
auth | permiso | Can change permission
auth | permiso | Can view permission
auth | usuario | Can add user
auth | usuario | Can change user
auth | usuario | Can view user
authtoken | Token | Can change Token
authtoken | Token | Can delete Token
Selecciona todos
Eliminar todos
GUARDAR
Guardar y añadir otro
Guardar y continuar editando
Eliminar
Inicio › Autenticación y autorización › Grupos › Eliminar múltiples objetos.
¿Está usted seguro que quiere eliminar el grupo seleccionado? Todos los siguientes objetos y sus elementos relacionados serán borrados:
Resumen
Grupos: 1
Relaciones group-permission: 6
Objetos
Grupo: Usuarios
Relación group-permission: Group_permissions object (81)
Relación group-permission: Group_permissions object (83)
Relación group-permission: Group_permissions object (84)
Relación group-permission: Group_permissions object (85)
Relación group-permission: Group_permissions object (86)
Relación group-permission: Group_permissions object (82)
Si, estoy seguro
No, llévame atrás

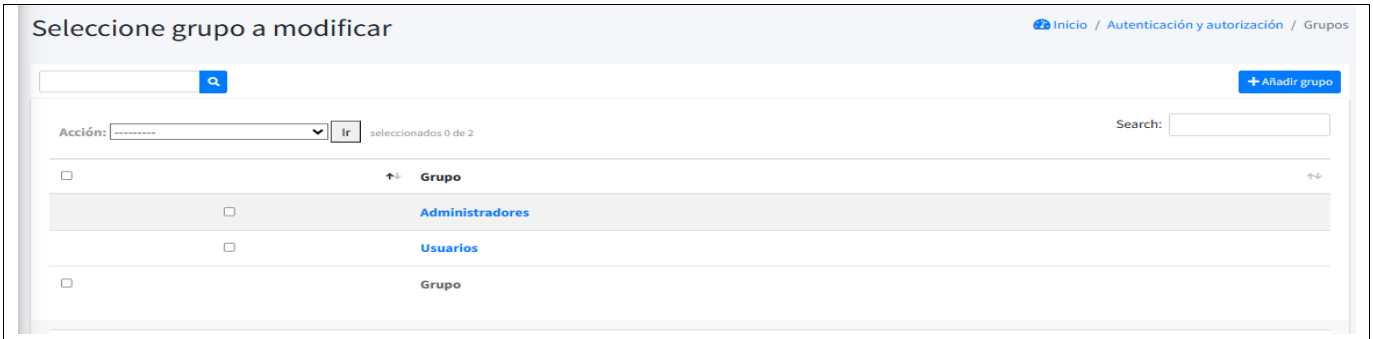
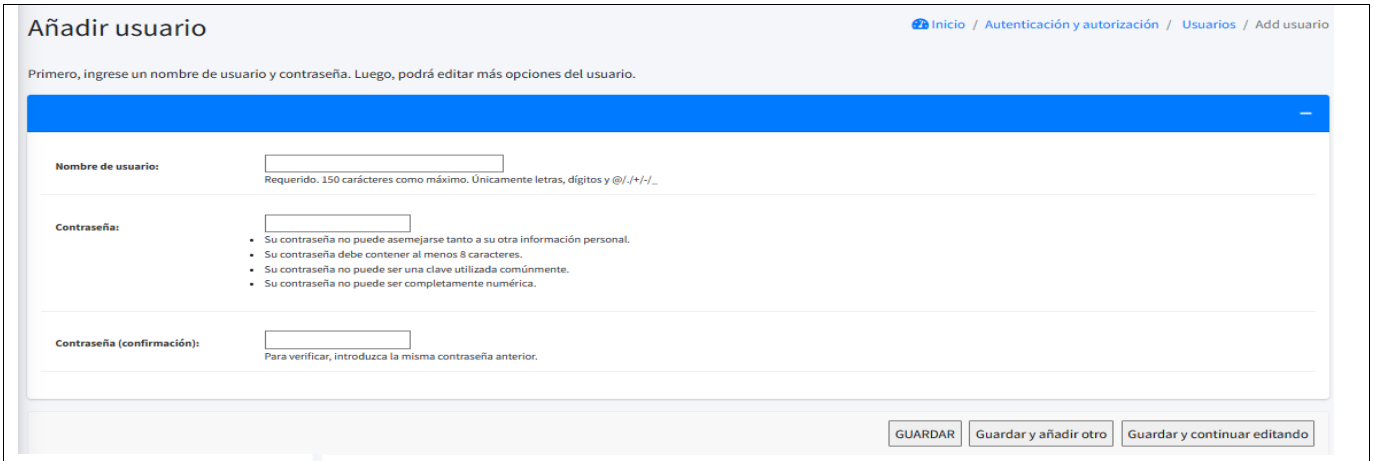
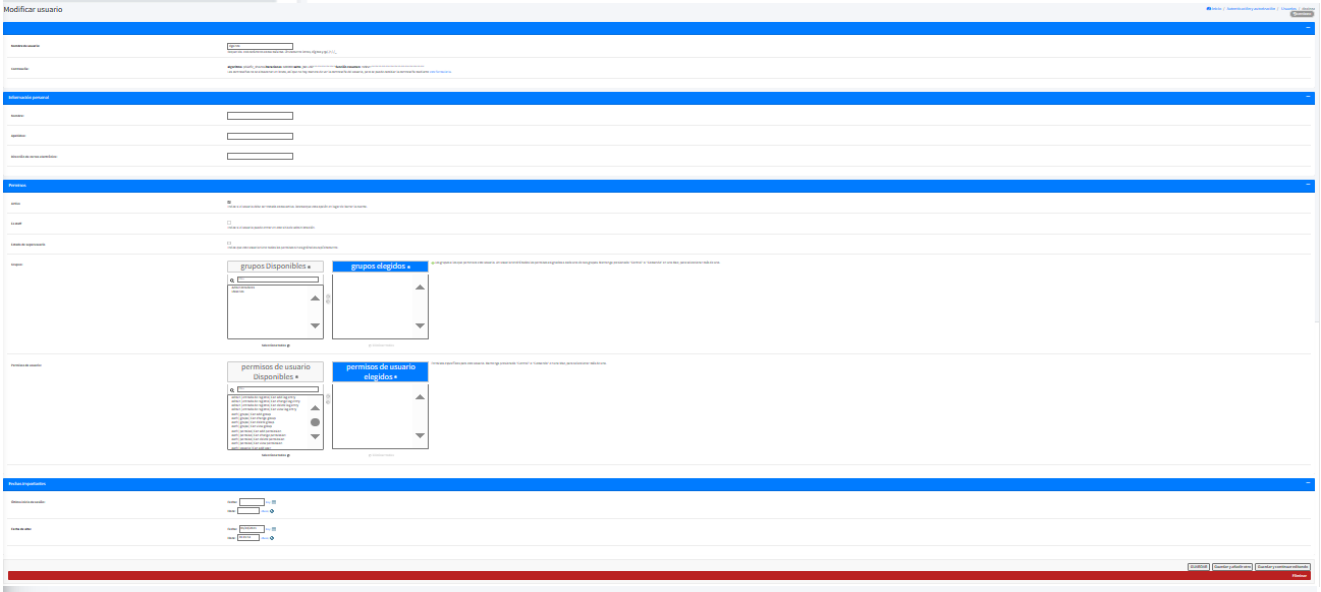


Tabla 50 Historia de Usuario #14

Historia de Usuario	
Número: HU_14	**Requisito:** Gestionar Usuario
Usuario: Administrador	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 0.3	**Iteración Asignada:** 2
Programador responsable: Yadira Sánchez Cruz	
Descripción: El administrador requiere gestionar los datos referentes los usuarios que interactúan con el sistema y se presentan las opciones de buscar, adicionar, modificar y eliminar. • **buscar usuario**: para ello, se teclea el nombre del usuario que se quiere buscar y como resultado se muestra el nombre del usuario, dirección de correo, nombre, apellido y si es del staff, en caso de no encontrarse el usuario se muestra que: "El usuario no fue encontrado" • **adicionar usuario**: para ello se introduce el nombre del usuario y la contraseña, al adicionarse se muestra un mensaje: El usuario "nombre del usuario" fue agregado correctamente. en caso de que exista el usuario se muestra que ya existe el usuario. • **modificar usuario**: para ello se busca el usuario que se quiere modificar y se cliquea sobre el mismo, se completan todos los datos del usuario (nombre, apellido, dirección de correo electrónico, permisos asociados y la fecha en que puede estar accediendo al sistema) al modificarse se muestra el mensaje: El usuario "nombre del usuario" se cambió correctamente. • **eliminar usuario**: para ello se selecciona el usuario que se quiere eliminar, antes de eliminarlo se emite el siguiente mensaje: ¿Está usted seguro que quiere eliminar el usuario seleccionado? Todos los siguientes objetos y sus elementos relacionados serán borrados, en caso de aceptar el sistema especifica lo siguiente: Eliminado/s 1 Usuario satisfactoriamente • **Filtrar:** se tiene la posibilidad además de poder filtrar los usuarios por grupo, si está activo, si es del staff y si es superusuario.	
Prototipo elemental de interfaz gráfica de usuario:	


Añadir usuario
Inicio / Autenticación y autorización / Usuarios / Add usuario
Primero, ingrese un nombre de usuario y contraseña. Luego, podrá editar más opciones del usuario.
Nombre de usuario:
Requerido. 150 carácteres como máximo. Únicamente letras, dígitos y @/./+/-/_
Contraseña:
Su contraseña no puede asemejarse tanto a su otra información personal.
Su contraseña debe contener al menos 8 caracteres.
Su contraseña no puede ser una clave utilizada comúnmente.
Su contraseña no puede ser completamente numérica.
Contraseña (confirmación):
Para verificar, introduzca la misma contraseña anterior.
GUARDAR
Guardar y añadir otro
Guardar y continuar editando

BUSCAR


Modificar usuario
grupos Disponibles
grupos elegidos
permisos de usuario Disponibles
permisos de usuario elegidos

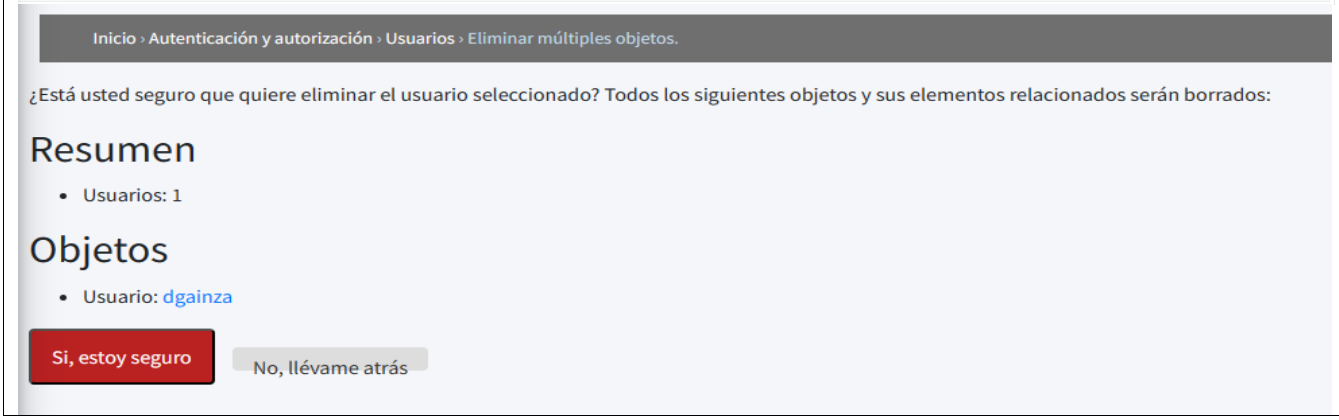
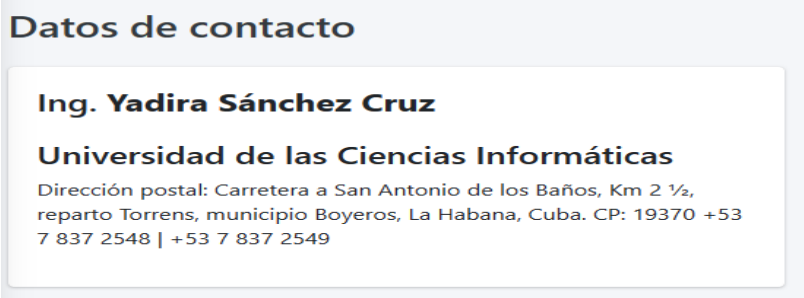

Inicio › Autenticación y autorización › Usuarios › Eliminar múltiples objetos.
¿Está usted seguro que quiere eliminar el usuario seleccionado? Todos los siguientes objetos y sus elementos relacionados serán borrados:
Resumen
Usuarios: 1
Objetos
Usuario: dgainza
Si, estoy seguro
No, llévame atrás

Tabla 51 Historia de Usuario #17

Historia de Usuario	
Número: HU_17	**Requisito:** Autenticar Usuario
Usuario: Usuario	
Prioridad en el negocio: Alta	**Riesgo en Desarrollo**: Medio
Puntos estimados: 0.3	**Iteración Asignada:** 2
Programador responsable: Yadira Sánchez Cruz	
Descripción: se le permite al usuario autenticarse en la aplicación para ello se le muestra una ventana en el navegador donde deben introducir su usuario y la contraseña	
Prototipo elemental de interfaz gráfica de usuario: 	

Tabla 52 Historia de Usuario #18

<table>
<tr><td colspan="3">Historia de Usuario</td></tr>
<tr><td>Número: HU_18</td><td colspan="2">Requisito: Datos de contacto</td></tr>
<tr><td colspan="3">Usuario: Usuario</td></tr>
<tr><td colspan="2">Prioridad en el negocio: Baja</td><td>Riesgo en Desarrollo: Baja</td></tr>
<tr><td colspan="2">Puntos estimados: 0.2</td><td>Iteración Asignada: 2</td></tr>
<tr><td colspan="3">Programador responsable: Yadira Sánchez Cruz</td></tr>
<tr><td colspan="3">Descripción: Muestra los datos de contactos del administrador (nombre y apellido, centro de trabajo, dirección, teléfono)</td></tr>
<tr><td colspan="3">Prototipo elemental de interfaz gráfica de usuario:
 
</td></tr>
</table>

Anexo 2. Tarjetas CRC

Tabla 53 Tarjeta CRC # 4

Tarjeta CRC	
Clase: DireccionIP	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes a las direcciones IP de los países atacantes. Siendo una clase Modelo o también conocida como Entidad.	Models Pais Admin DireccionIPVisualizacion

Tabla 54 Tarjeta CRC # 5

Tarjeta CRC	
Clase: Tecnología	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes a la tecnología atacada. Siendo una clase Modelo o también conocida como Entidad.	Models Admin TecnologiaVisualizacion

Tabla 55 Tarjeta CRC # 6

Tarjeta CRC	
Clase: ClasificacionIncidente	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes a la clasificación del incidente ocurrido. Siendo una clase Modelo o también conocida como Entidad.	Models Admin ClasificacionIncidenteBuscador

Tabla 56 Tarjeta CRC # 7

Tarjeta CRC	
Clase: Entidad	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes a la entidad atacada. Siendo una clase Modelo o también conocida como Entidad.	Models Admin EntidadBuscador

Tabla 57 Tarjeta CRC # 9

Tarjeta CRC	
Clase: MetodoHTTP	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes método HTTP utilizado para realizar la petición. Siendo una clase Modelo o también conocida como Entidad.	Models Admin MetodoHTTPVisualizacion

Tabla 58 Tarjeta CRC # 10

Tarjeta CRC

Clase: CodigoRespuestaHTTP	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes al código de respuesta HTTP proporcionada. Siendo una clase Modelo o también conocida como Entidad.	Models Admin CodigoRespuestaHTTPVisualizacion

Tabla 59 Tarjeta CRC # 11

Tarjeta CRC	
Clase: AgenteUsuario	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes al agente de usuario utilizado para la petición. Siendo una clase Modelo o también conocida como Entidad.	Models Admin AgenteUsuarioVisualizacion

Tabla 60 Tarjeta CRC # 12

Tarjeta CRC	
Clase: Referencia	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes a la referencia de la petición. Siendo una clase Modelo o también conocida como Entidad.	Models Admin ReferenciaVisualizacion

Tabla 61 Tarjeta CRC # 13

Tarjeta CRC	
Clase: URL	
Responsabilidades	Colaboraciones
Representar los datos persistentes en la base de datos correspondientes a la dirección URL utilizada para la petición. Siendo una clase Modelo o también conocida como Entidad.	Models Admin URLVisualizacion

Tabla 62 Tarjeta CRC # 16

Tarjeta CRC	
Clase: DireccionIPVizualizacion	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar la dirección IP sospechosa	Admin

Tabla 63 Tarjeta CRC # 17

Tarjeta CRC	
Clase: ClasificacionIncidenteBuscador	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar un incidente de seguridad.	Admin

Tabla 64 Tarjeta CRC # 18

Tarjeta CRC	
Clase: EntidadBuscador	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar la entidad a la que se envía la petición sospechosa.	Admin

Tabla 65 Tarjeta CRC # 19

Tarjeta CRC	
Clase: TecnologiaVisualizacion	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar la tecnología explotada para realizar la petición sospechosa.	Admin

Tabla 66 Tarjeta CRC # 20

Tarjeta CRC	
Clase: IncidenteBuscador	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar el incidente de seguridad provocado por la petición IP maliciosa	Admin

Tabla 67 Tarjeta CRC # 21

Tarjeta CRC	
Clase: MetodoHTTPVisualizacion	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar el método HTTP utilizado para realizar la petición sospechosa	Admin

Tabla 68 Tarjeta CRC # 22

Tarjeta CRC	
Clase: CodigoRespuestaHTTPVisualizacion	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar el código de respuesta HTTP emitido	Admin

Tabla 69 Tarjeta CRC # 23

Tarjeta CRC	
Clase: AgenteUsuarioVisualizacion	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones	Admin

orientadas a gestionar el agente de usuario	

Tabla 70 Tarjeta CRC # 24

Tarjeta CRC	
Clase: ReferenciaVisualizacion	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar la referencia de la petición sospechosa	Admin

Tabla 71 Tarjeta CRC # 25

Tarjeta CRC	
Clase: URLVisualizacion	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar la URL de la petición sospechosa	Admin

Tabla 72 Tarjeta CRC # 26

Tarjeta CRC	
Clase: PeticionVisualizacion	
Responsabilidades	Colaboraciones
renderiza la vista para especificar las configuraciones orientadas a gestionar los datos de la petición sospechosa realizada	Admin

Anexo 3. Tareas de Ingeniería

Iteración 1

Tabla 73 Tarea de ingeniería 5

Tarea de Ingeniería	
Número de la tarea: 5	**Número de Historia de Usuario:** 5
Nombre de la tarea: Visualización de los datos del agente du usuario	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 23/03/2023	**Fecha de fin:** 27/03/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase AgenteUsuario que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar un agente de usuario	

Tabla 74 Tarea de ingeniería 6

Tarea de Ingeniería	
Número de la tarea: 6	**Número de Historia de Usuario:** 6
Nombre de la tarea: Visualización de los datos de la referencia	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 28/03/2023	**Fecha de fin:** 30/03/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase Referencia que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar una referencia.	

Tabla 75 Tarea de ingeniería 7

Tarea de Ingeniería	
Número de la tarea: 7	**Número de Historia de Usuario:** 1 a la 14
Nombre de la tarea: Configurar las vistas proporcionadas por el framework de desarrolla Django para visualizar los CRUD de la aplicación	
Tipo de tarea: Desarrollo	**Puntos estimados:** 2
Fecha de inicio: 03/04/2023	**Fecha de fin:** 13/04/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se deben configurar las plantillas proporcionadas por el framework de desarrollo usado para poder tener una personalización de las mismas y que muestren lo que desea el cliente. Esta tarea es general para todas las HU que realizan un CRUD.	

Iteración 2

Tabla 76 Tarea de ingeniería 8

Tarea de Ingeniería	
Número de la tarea: 8	**Número de Historia de Usuario:** 7
Nombre de la tarea: Visualización de los datos de la URL	

Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 17/04/2023	**Fecha de fin:** 19/04/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase URL que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar la URL por la cual se emitió la petición sospechosa	

Tabla 77 Tarea de ingeniería 9

Tarea de Ingeniería	
Número de la tarea: 9	**Número de Historia de Usuario:** 8
Nombre de la tarea: Visualización de los datos de la tecnología atacada	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 20/04/2023	**Fecha de fin:** 24/04/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase Tecnologia que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar la tecnología atacada.	

Tabla 78 Tarea de ingeniería 10

Tarea de Ingeniería	
Número de la tarea: 10	**Número de Historia de Usuario:** 9
Nombre de la tarea: Visualización de los datos de la clasificación del incidente	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 25/04/2023	**Fecha de fin:** 27/04/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase ClasificacionIncidente que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar una clasificación del incidente.	

Tabla 79 Tarea de ingeniería 11

Tarea de Ingeniería	
Número de la tarea: 11	**Número de Historia de Usuario:** 10
Nombre de la tarea: Visualización de los datos de la entidad atacada	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 02/05/2023	**Fecha de fin:** 04/05/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite configurar los datos que debe mostrar la clase Entidad que hereda de admin.py cuando realice las funcionalidades de crear, listar, modificar y eliminar una entidad atacada	

Tabla 80 Tarea de ingeniería 15

Tarea de Ingeniería	
Número de la tarea: 15	**Número de Historia de Usuario:** 15
Nombre de la tarea: Visualizar reporte de las últimas URL atacadas	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 25/05/2023	**Fecha de fin:** 29/05/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite mostrar las últimas 10 URL atacadas registradas en el sistema, mostrando una lista con las URL que hayan sido atacadas y estén registradas en el sistema en los últimos días	

Tabla 81 Tarea de ingeniería 16

Tarea de Ingeniería	
Número de la tarea: 16	**Número de Historia de Usuario:** 15
Nombre de la tarea: Visualizar reporte de los últimos códigos de respuestas generados por los ataques	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 30/05/2023	**Fecha de fin:** 01/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite mostrar los últimos 10 códigos de respuesta que se han generado al recibir peticiones sospechosas, mostrando una lista con los códigos de respuestas generados en los últimos días	

Tabla 82 Tarea de ingeniería 17

Tarea de Ingeniería	
Número de la tarea: 17	**Número de Historia de Usuario:** 15
Nombre de la tarea: Visualizar reporte de los últimos países atacantes	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 05/06/2023	**Fecha de fin:** 06/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite mostrar los últimos 10 países atacantes, mostrando una lista de los países que han realizado peticiones sospechosas en los últimos días	

Tabla 83 Tarea de ingeniería 18

Tarea de Ingeniería	
Número de la tarea: 18	**Número de Historia de Usuario:** 15
Nombre de la tarea: Visualizar reporte de los últimos métodos HTTP utilizados para realizar las peticiones sospechosas	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 07/06/2023	**Fecha de fin:** 08/06/2023
Programador responsable: Yadira Sánchez Cruz	

Descripción:
Se implementa una funcionalidad que permite mostrar los últimos 10 métodos HTTP utilizados para realizar las peticiones sospechosas, mostrando una lista de los métodos HTTP que han usado para realizar peticiones sospechosas en los últimos días

Tabla 84 Tarea de ingeniería 19

Tarea de Ingeniería	
Número de la tarea: 19	**Número de Historia de Usuario:** 15
Nombre de la tarea: Visualizar reporte de los últimos agentes de usuario utilizados	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 05/06/2023	**Fecha de fin:** 06/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite mostrar los últimos 10 agentes de usuarios utilizados, mostrando una lista de los agentes de usuarios que han utilizado para realizar peticiones sospechosas en los últimos días	

Tabla 85 Tarea de ingeniería 22

Tarea de Ingeniería	
Número de la tarea: 22	**Número de Historia de Usuario:** 16
Nombre de la tarea: Generar gráfico de principales URL atacadas	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 14/06/2023	**Fecha de fin:** 15/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite generar un gráfico donde se muestre cuáles han sido las principales URL atacadas, teniendo en cuenta la cantidad de peticiones enviada a las mismas.	

Tabla 86 Tarea de ingeniería 23

Tarea de Ingeniería	
Número de la tarea: 23	**Número de Historia de Usuario:** 16
Nombre de la tarea: Generar gráfico de principales clasificaciones de incidente	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 19/06/2023	**Fecha de fin:** 20/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite generar un gráfico donde se muestre cuáles han sido las principales clasificaciones de incidentes, teniendo en cuenta el tipo de incidente recibido y la cantidad de veces que se ha recibido.	

Tabla 87 Tarea de ingeniería 24

Tarea de Ingeniería	
Número de la tarea: 24	**Número de Historia de Usuario:** 16
Nombre de la tarea: Generar gráfico de las principales tecnologías atacadas	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2

Fecha de inicio: 05/06/2023	**Fecha de fin:** 06/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite generar un gráfico donde se muestre cuáles han sido las principales tecnologías atacadas, teniendo en cuenta la cantidad de veces que se ha recibido ataque dicha tecnología.	

Tabla 88 Tarea de ingeniería 25

Tarea de Ingeniería	
Número de la tarea: 25	**Número de Historia de Usuario:** 16
Nombre de la tarea: Generar gráfico de principales métodos HTTP usados para realizar la petición sospechosa	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 14/06/2023	**Fecha de fin:** 15/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite generar un gráfico donde se muestre cuáles han sido los principales métodos HTTP usados para realizar peticiones sospechosas, teniendo en cuenta la cantidad de veces que se ha utilizado el mismo para ello.	

Tabla 89 Tarea de ingeniería 26

Tarea de Ingeniería	
Número de la tarea: 26	**Número de Historia de Usuario:** 17
Nombre de la tarea: Autenticar Usuario	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 14/06/2023	**Fecha de fin:** 15/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite a los usuarios autenticarse en el sistema.	

Tabla 90 Tarea de ingeniería 27

Tarea de Ingeniería	
Número de la tarea: 27	**Número de Historia de Usuario:** 18
Nombre de la tarea: Datos de contacto	
Tipo de tarea: Desarrollo	**Puntos estimados:** 0.2
Fecha de inicio: 14/06/2023	**Fecha de fin:** 15/06/2023
Programador responsable: Yadira Sánchez Cruz	
Descripción: Se implementa una funcionalidad que permite introducir los datos de contacto de la persona que administra el proyecto para luego poder ser mostrados.	

Anexo 4. Casos de Prueba de Aceptación

Iteración 1

Tabla 91 Prueba de Aceptación 6

Caso de prueba de aceptación	
Código: HU2_P1	**Historia de usuario:** 2
Nombre: Adicionar una dirección IP	
Descripción: Prueba para la funcionalidad Gestionar Dirección IP, en este caso para Adicionar dirección IP (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La dirección IP no debe verse adicionado anteriormente	
Pasos de ejecución: 5. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*IP'* 6. El usuario selecciona dentro de las opciones del módulo IP la opción '*Direcciones IP*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la dirección IP. 7. El usuario selecciona dentro de la vista el botón '*Anadir Dirección IP*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la dirección IP 8. El usuario completa el campo 'Dirección IP 'y se selecciona el país del que procede y selecciona cualquiera de los tres botones que aparecen en el formulario: d. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de direcciones IP con la dirección IP agregada al final de la lista e. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó la dirección IP correctamente y se mantiene en el formulario para poder adicionar una nueva dirección IP f. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó la dirección IP correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la dirección IP	
Evaluación de la prueba: Satisfactoria	

Tabla 92 Prueba de Aceptación 7

Caso de prueba de aceptación	
Código: HU2_P2	**Historia de usuario:** 2
Nombre: Adicionar una dirección IP	
Descripción: Prueba para la funcionalidad Gestionar Dirección IP, en este caso para Adicionar dirección IP (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La dirección IP no debe verse adicionado anteriormente.	
Pasos de ejecución: 6. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*IP'* 7. El usuario selecciona dentro de las opciones del módulo IP la opción '*Direcciones IP*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la dirección IP. 8. El usuario selecciona dentro de la vista el botón '*Anadir Dirección IP*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la dirección IP 9. El usuario completa el campo 'dirección IP 'en el formulario introduciendo datos erróneos para la dirección IP, o una dirección IP que ya existe y selecciona cualquiera de los tres botones que aparecen en el formulario. 10. EL sistema muestra mensajes de Introduzca una dirección IPv4 o IPv6 válida, o ya existe una dirección IP con esa descripción	
Evaluación de la prueba: No Satisfactoria	

Tabla 93 Prueba de Aceptación 8

Caso de prueba de aceptación	
Código: HU2_P3	**Historia de usuario:** 2
Nombre: Modificar una dirección IP	
Descripción: Prueba para la funcionalidad Gestionar Dirección IP, en este caso para Modificar una dirección IP	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La dirección IP debe existir en el sistema	
Pasos de ejecución: 5. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*IP'* 6. El usuario selecciona dentro de las opciones del módulo IP la opción '*Direcciones IP*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la dirección IP. 7. El usuario debe pinchar sobre la dirección IP que quiere modificar y el sistema debe llevarlo a la vista de Adicionar dirección IP, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar la dirección IP 8. El usuario modifica el campo 'dirección IP 'en el formulario, este dato debe cumplir con las normativas de las direcciones IPv4 e IPv6 y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de las direcciones IP con la dirección IP agregada al final de la lista y un mensaje diciendo que la dirección IP fue modificada correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió la dirección IP correctamente y se mantiene en el formulario para poder adicionar una nueva dirección IP c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió la dirección IP correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la dirección IP d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados a la dirección IP que se quiere eliminar y da dos opciones (si quiere eliminar la dirección IP, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 94 Prueba de Aceptación 9

Caso de prueba de aceptación	
Código: HU2_P4	**Historia de usuario:** 2
Nombre: Eliminar dirección IP	
Descripción: Prueba para la funcionalidad Gestionar Dirección IP, en este caso para eliminar una dirección IP	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La dirección IP debe existir en el sistema	
Pasos de ejecución: 4. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*IP'* 5. El usuario selecciona dentro de las opciones del módulo IP la opción '*Direcciones IP*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la dirección IP. 6. El usuario selecciona la dirección IP que quiere eliminar marcando el cuadro que aparece delante del identificador, busca la acción eliminar dirección IP seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados a la dirección IP y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina la dirección IP con todos los elementos asociados a ella y muestra el mensaje se eliminó 1 dirección IP satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de las direcciones IP	
Evaluación de la prueba: Satisfactoria	

Tabla 95 Prueba de Aceptación 10

Caso de prueba de aceptación	
Código: HU2_P5	**Historia de usuario:** 2
Nombre: Buscar dirección IP	
Descripción: Prueba para la funcionalidad Gestionar Dirección IP, en este caso para Buscar una dirección IP	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La dirección IP debe existir en el sistema	
Pasos de ejecución: 4. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*IP'* 5. El usuario selecciona dentro de las opciones del módulo IP la opción '*Direcciones IP*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la dirección IP. 6. El usuario escribe la dirección IP que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con la dirección IP seleccionada, en caso de no encontrarse debe mostrar el mensaje de que la dirección IP no fue encontrada	
Evaluación de la prueba: Satisfactoria	

Tabla 96 Prueba de Aceptación 11

Caso de prueba de aceptación	
Código: HU8_P1	**Historia de usuario:** 8
Nombre: Adicionar una tecnología	
Descripción: Prueba para la funcionalidad Gestionar Tecnología, en este caso para Adicionar una tecnología (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La tecnología no debe verse adicionado anteriormente	
Pasos de ejecución: 9. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 10. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*Tecnologías*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la tecnología. 11. El usuario selecciona dentro de la vista el botón '*Anadir Tecnología*, el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la tecnología 12. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 70 y selecciona cualquiera de los tres botones que aparecen en el formulario: g. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de tecnologías con la tecnología agregada al final de la lista h. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó la tecnología correctamente y se mantiene en el formulario para poder adicionar una nueva tecnología i. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó la tecnología correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la tecnología	
Evaluación de la prueba: Satisfactoria	

Tabla 97 Prueba de Aceptación 12

Caso de prueba de aceptación	
Código: HU8_P3	**Historia de usuario:** 8
Nombre: Modificar una tecnología	
Descripción: Prueba para la funcionalidad Gestionar Tecnología, en este caso para Modificar una tecnología	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La tecnología debe existir en el sistema	
Pasos de ejecución: 9. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 10. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*Tecnologías*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la tecnología. 11. El usuario debe pinchar sobre la tecnología que quiere modificar y el sistema debe llevarlo a la vista de Adicionar tecnología, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar la tecnología 12. El usuario modifica el campo 'descripción 'en el formulario, este dato debe ser una cadena de caracteres y aceptar hasta 70 caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de os tecnologías con la tecnología agregado al final de la lista y un mensaje diciendo que la tecnología fue modificada correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió la tecnología correctamente y se mantiene en el formulario para poder adicionar una nueva tecnología c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió la tecnología correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la tecnología d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados a la tecnología que se quiere eliminar y da dos opciones (si quiere eliminar la tecnología, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 98 Prueba de Aceptación 13

Caso de prueba de aceptación	
Código: HU8_P4	**Historia de usuario:** 8
Nombre: Eliminar tecnología	
Descripción: Prueba para la funcionalidad Gestionar Tecnología, en este caso para eliminar una tecnología	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La tecnología debe existir en el sistema	
Pasos de ejecución: 7. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 8. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*Tecnologías*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la tecnología. 9. El usuario selecciona la tecnología que quiere eliminar marcando el cuadro que aparece delante del identificador, busca la acción eliminar tecnología seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados al tecnología y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina la tecnología con todos los elementos asociados a él y muestra el mensaje se eliminó 1 Tecnología satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de las tecnologías	
Evaluación de la prueba: Satisfactoria	

Tabla 99 Prueba de Aceptación 14

Caso de prueba de aceptación	
Código: HU8_P5	**Historia de usuario:** 8
Nombre: Buscar tecnología	
Descripción: Prueba para la funcionalidad Gestionar Tecnología, en este caso para Buscar una tecnología	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La tecnología debe existir en el sistema	
Pasos de ejecución: 7. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 8. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*Tecnologías*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la tecnología. 9. El usuario escribe la descripción de la tecnología que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con la tecnología seleccionado, en caso de no encontrarse debe mostrar el mensaje de que la tecnología no fue encontrada	
Evaluación de la prueba: Satisfactoria	

Tabla 100 Prueba de Aceptación 15

Caso de prueba de aceptación	
Código: HU9_P1	**Historia de usuario:** 9
Nombre: Adicionar una clasificación del incidente	
Descripción: Prueba para la funcionalidad Gestionar clasificación del incidente, en este caso para Adicionar clasificación del incidente (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La clasificación del incidente no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción 'C*lasificaciones de Incidentes*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la clasificación del incidente. 3. El usuario selecciona dentro de la vista el botón '*Anadir clasificación del incidente*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la clasificación del incidente 4. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 90 y selecciona cualquiera de los tres botones que aparecen en el formulario: a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de clasificación del incidente con la clasificación del incidente agregada al final de la lista b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó la clasificación del incidente correctamente y se mantiene en el formulario para poder adicionar una nueva clasificación del incidente c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó la clasificación del incidente correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la clasificación del incidente	
Evaluación de la prueba: Satisfactoria	

Tabla 101 Prueba de Aceptación 16

Caso de prueba de aceptación	
Código: HU9_P2	**Historia de usuario:** 9
Nombre: Adicionar una clasificación del incidente	
Descripción: Prueba para la funcionalidad Gestionar clasificación del incidente, en este caso para adicionar clasificación del incidente (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La clasificación del incidente no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción 'C*lasificaciones de Incidentes*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de una clasificación del incidente. 3. El usuario selecciona dentro de la vista el botón '*Anadir clasificación del incidente*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la clasificación del incidente 4. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de una clasificación del incidente que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 5. El sistema muestra mensajes de error de ya existe una clasificación del incidente con ese nombre o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 102 Prueba de Aceptación 17

Caso de prueba de aceptación	
Código: HU9_P3	**Historia de usuario:** 9
Nombre: Modificar una clasificación del incidente	
Descripción: Prueba para la funcionalidad Gestionar clasificación del incidente, en este caso para modificar una clasificación del incidente	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La clasificación del incidente debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción 'C*lasificaciones de incidentes*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la clasificación del incidente. 3. El usuario debe pinchar sobre la descripción de la clasificación del incidente que quiere modificar y el sistema debe llevarlo a la vista de adicionar clasificación del incidente, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar la clasificación del incidente 4. El usuario modifica el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 90 y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de clasificación del incidente con la clasificación del incidente agregada al final de la lista y un mensaje diciendo que la clasificación del incidente fue modificada correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió la clasificación del incidente correctamente y se mantiene en el formulario para poder adicionar una nueva clasificación del incidente c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió la clasificación del incidente correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar la clasificación del incidente d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados a la CLASIFICACIÓN DEL INCIDENTE que se quiere eliminar y da dos opciones (si quiere eliminar la CLASIFICACIÓN DEL INCIDENTE, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 103 Prueba de Aceptación 18

Caso de prueba de aceptación	
Código: HU9_P5	**Historia de usuario:** 9
Nombre: Buscar clasificación del incidente	
Descripción: Prueba para la funcionalidad Gestionar clasificación del incidente, en este caso para buscar una clasificación del incidente	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La clasificación del incidente debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción 'C*lasificaciones de incidentes*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la clasificación del incidente. 3. El usuario escribe el nombre del país que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con la clasificación del incidente seleccionada, en caso de no encontrarse debe mostrar el mensaje de que la clasificación del incidente no fue encontrada	
Evaluación de la prueba: Satisfactoria	

Tabla 104 Prueba de Aceptación 19

Caso de prueba de aceptación	
Código: HU10_P1	**Historia de usuario:** 10
Nombre: Adicionar una entidad	
Descripción: Prueba para la funcionalidad Gestionar Entidad, en este caso para Adicionar una entidad (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La entidad no debe verse adicionado anteriormente	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*Entidades*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la entidad. 3. El usuario selecciona dentro de la vista el botón '*Anadir Entidad*, el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la entidad 4. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 90 y selecciona cualquiera de los tres botones que aparecen en el formulario: j. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de entidades con la entidad agregada al final de la lista k. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó la entidad correctamente y se mantiene en el formulario para poder adicionar una nueva entidad l. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó la entidad correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la entidad	
Evaluación de la prueba: Satisfactoria	

Tabla 105 Prueba de Aceptación 20

Caso de prueba de aceptación	
Código: HU10_P2	**Historia de usuario:** 10
Nombre: Adicionar entidad	
Descripción: Prueba para la funcionalidad Gestionar Entidad, en este caso para Adicionar entidad (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La entidad no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*Entidades*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la entidad. 3. El usuario selecciona dentro de la vista el botón '*Anadir Entidad*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la entidad 4. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de una entidad que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 5. El sistema muestra mensajes de error de ya existe una entidad con esa descripción o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 106 Prueba de Aceptación 21

Caso de prueba de aceptación	
Código: HU10_P3	**Historia de usuario:** 10
Nombre: Modificar una entidad	
Descripción: Prueba para la funcionalidad Gestionar Entidad, en este caso para Modificar una entidad	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La entidad debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*Entidades*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la entidad. 3. El usuario debe pinchar sobre la entidad que quiere modificar y el sistema debe llevarlo a la vista de Adicionar entidad, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar la entidad 4. El usuario modifica el campo 'descripción 'en el formulario, este dato debe ser una cadena de caracteres y aceptar hasta 90 caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de os entidades con la entidad agregado al final de la lista y un mensaje diciendo que la entidad fue modificada correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió la entidad correctamente y se mantiene en el formulario para poder adicionar una nueva entidad c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió la entidad correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la entidad d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados a la entidad que se quiere eliminar y da dos opciones (si quiere eliminar la entidad, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 107 Prueba de Aceptación 22

Caso de prueba de aceptación	
Código: HU10_P4	**Historia de usuario:** 10
Nombre: Eliminar entidad	
Descripción: Prueba para la funcionalidad Gestionar Entidad, en este caso para eliminar una entidad	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La entidad debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*Entidades*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la entidad. 3. El usuario selecciona la entidad que quiere eliminar marcando el cuadro que aparece delante del identificador, busca la acción eliminar entidad seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados al entidad y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina la entidad con todos los elementos asociados a él y muestra el mensaje se eliminó 1 Entidad satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de las entidades	
Evaluación de la prueba: Satisfactoria	

Tabla 108 Prueba de Aceptación 23

Caso de prueba de aceptación	
Código: HU10_P5	**Historia de usuario:** 10
Nombre: Buscar entidad	
Descripción: Prueba para la funcionalidad Gestionar Entidad, en este caso para Buscar una entidad	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La entidad debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*Entidades*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la entidad. 3. El usuario escribe la descripción de la entidad que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con la entidad seleccionado, en caso de no encontrarse debe mostrar el mensaje de que la entidad no fue encontrada	
Evaluación de la prueba: Satisfactoria	

Tabla 109 Prueba de Aceptación 24

Caso de prueba de aceptación	
Código: HU11_P1	**Historia de usuario:** 11
Nombre: Adicionar un incidente	
Descripción: Prueba para la funcionalidad Gestionar incidente, en este caso para Adicionar incidente (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El incidente no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción 'Incidentes' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos del incidente. 3. El usuario selecciona dentro de la vista el botón '*Anadir incidente*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del incidente 4. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 112 y selecciona cualquiera de los tres botones que aparecen en el formulario: a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de incidente con el incidente agregada al final de la lista b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó el incidente correctamente y se mantiene en el formulario para poder adicionar un nuevo incidente c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó el incidente correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar el incidente	
Evaluación de la prueba: Satisfactoria	

Tabla 110 Prueba de Aceptación 25

Caso de prueba de aceptación	
Código: HU11_P2	**Historia de usuario:** 11
Nombre: Adicionar un incidente	
Descripción: Prueba para la funcionalidad Gestionar incidente, en este caso para adicionar incidente (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El incidente no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción 'Incidentes' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de un incidente. 3. El usuario selecciona dentro de la vista el botón '*Anadir incidente*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del incidente 4. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de un incidente que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 5. El sistema muestra mensajes de error de ya existe un incidente con ese nombre o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 111 Prueba de Aceptación 26

Caso de prueba de aceptación	
Código: HU11_P3	**Historia de usuario:** 11
Nombre: Modificar un incidente	
Descripción: Prueba para la funcionalidad Gestionar incidente, en este caso para modificar un incidente	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El incidente debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción 'Incidentes' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del incidente. 3. El usuario debe pinchar sobre la descripción del incidente que quiere modificar y el sistema debe llevarlo a la vista de adicionar incidente, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar el incidente 4. El usuario modifica el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 112 y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de incidente con el incidente agregada al final de la lista y un mensaje diciendo que el incidente fue modificado correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió el incidente correctamente y se mantiene en el formulario para poder adicionar un nuevo incidente c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió el incidente correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar el incidente d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados a el incidente que se quiere eliminar y da dos opciones (si quiere eliminar el incidente, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 112 Prueba de Aceptación 27

Caso de prueba de aceptación	
Código: HU11_P4	**Historia de usuario:** 11
Nombre: Eliminar un incidente	
Descripción: Prueba para la funcionalidad Gestionar incidente, en este caso para eliminar un incidente	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El incidente debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción *'Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*incidentes*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del incidente. 3. El usuario selecciona el incidente que quiere eliminar marcando el cuadro que aparece delante del identificar, busca la acción eliminar incidente seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados a el incidente y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina el incidente con todos los elementos asociados a él y muestra el mensaje se eliminó 1 incidente satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de las clasificaciones de incidente	
Evaluación de la prueba: Satisfactoria	

Iteración 2

Tabla 113 Prueba de Aceptación 28

Caso de prueba de aceptación	
Código: HU3_P1	**Historia de usuario:** 3
Nombre: Adicionar un método HTTP	
Descripción: Prueba para la funcionalidad Gestionar Método HTTP, en este caso para Adicionar método HTTP (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El método HTTP no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Métodos HTTP*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos del método HTTP. 3. El usuario selecciona dentro de la vista el botón '*Anadir Método HTTP*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del método HTTP 4. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 50 y selecciona cualquiera de los tres botones que aparecen en el formulario: a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de métodos HTTP con el método HTTP agregado al final de la lista b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó el método HTTP correctamente y se mantiene en el formulario para poder adicionar un nuevo método HTTP c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó el método HTTP correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar el método HTTP	
Evaluación de la prueba: Satisfactoria	

Tabla 114 Prueba de Aceptación 29

Caso de prueba de aceptación	
Código: HU3_P2	**Historia de usuario:** 3
Nombre: Adicionar un Método HTTP	
Descripción: Prueba para la funcionalidad Gestionar Método HTTP, en este caso para Adicionar método HTTP (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El método HTTP no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Métodos HTTP*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de un método HTTP. 3. El usuario selecciona dentro de la vista el botón '*Anadir Método HTTP*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del método HTTP 4. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de un método HTTP que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 5. El sistema muestra mensajes de error de ya existe un método HTTP con ese nombre o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 115 Prueba de Aceptación 30

Caso de prueba de aceptación	
Código: HU3_P3	**Historia de usuario:** 3
Nombre: Modificar un método HTTP	
Descripción: Prueba para la funcionalidad Gestionar Método HTTP, en este caso para Modificar un método HTTP	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El método HTTP debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Métodos HTTP*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del método HTTP. 3. El usuario debe pinchar sobre la descripción del método HTTP que quiere modificar y el sistema debe llevarlo a la vista de Adicionar Método HTTP, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar el Método HTTP 4. El usuario modifica el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 50 y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de métodos HTTP con el método HTTP agregado al final de la lista y un mensaje diciendo que el método HTTP fue modificado correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió el método HTTP correctamente y se mantiene en el formulario para poder adicionar un nuevo método HTTP c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió el método HTTP correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar el método HTTP d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados al método HTTP que se quiere eliminar y da dos opciones (si quiere eliminar el Método HTTP, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 116 Prueba de Aceptación 31

Caso de prueba de aceptación	
Código: HU3_P4	**Historia de usuario:** 3
Nombre: Eliminar un Método HTTP	
Descripción: Prueba para la funcionalidad Gestionar Método HTTP, en este caso para eliminar un método HTTP	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El método HTTP debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción *'Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Métodos HTTP*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del método HTTP. 3. El usuario selecciona el método HTTP que quiere eliminar marcando el cuadro que aparece delante del identificar, busca la acción eliminar método HTTP seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados al método HTTP y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina el método HTTP con todos los elementos asociados a él y muestra el mensaje se eliminó 1 Método HTTP satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de los métodos HTTP	
Evaluación de la prueba: Satisfactoria	

Tabla 117 Prueba de Aceptación 32

Caso de prueba de aceptación	
Código: HU3_P5	**Historia de usuario:** 3
Nombre: Buscar método HTTP	
Descripción: Prueba para la funcionalidad Gestionar Método HTTP, en este caso para Buscar un método HTTP	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El método HTTP debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Métodos HTTP*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del método HTTP. 3. El usuario escribe el nombre del país que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con el método HTTP seleccionado, en caso de no encontrarse debe mostrar el mensaje de que el método HTTP no fue encontrado	
Evaluación de la prueba: Satisfactoria	

Tabla 118 Prueba de Aceptación 33

Caso de prueba de aceptación	
Código: HU4_P1	**Historia de usuario:** 4
Nombre: Adicionar un código de respuesta HTTP	
Descripción: Prueba para la funcionalidad Gestionar Código de Respuesta HTTP, en este caso para Adicionar un código de respuesta HTTP (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El código de respuesta HTTP no debe verse adicionado anteriormente	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Códigos de Respuesta HTTP*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos del código de respuesta HTTP. 3. El usuario selecciona dentro de la vista el botón '*Anadir Código de Respuesta HTTP*, el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del código de respuesta HTTP 4. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 50 y selecciona cualquiera de los tres botones que aparecen en el formulario: m. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de códigos de respuestas HTTP con el código de respuesta HTTP agregada al final de la lista n. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó el código de respuesta HTTP correctamente y se mantiene en el formulario para poder adicionar un nuevo código de respuesta HTTP o. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó el código de respuesta HTTP correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar el código de respuesta HTTP	
Evaluación de la prueba: Satisfactoria	

Tabla 119 Prueba de Aceptación 34

Caso de prueba de aceptación	
Código: HU4_P2	**Historia de usuario:** 4
Nombre: Adicionar código de respuesta HTTP	
Descripción: Prueba para la funcionalidad Gestionar Código de Respuesta HTTP, en este caso para Adicionar código de respuesta HTTP (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El código de respuesta HTTP no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Códigos de Respuesta HTTP*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos del código de respuesta HTTP. 3. El usuario selecciona dentro de la vista el botón '*Anadir Código de respuesta HTTP*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del código de respuesta HTTP 4. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de un código de respuesta HTTP que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 5. El sistema muestra mensajes de error de ya existe un código de respuesta HTTP con esa descripción o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 120 Prueba de Aceptación 35

Caso de prueba de aceptación	
Código: HU4_P3	**Historia de usuario:** 4
Nombre: Modificar un código de respuesta HTTP	
Descripción: Prueba para la funcionalidad Gestionar Código de Respuesta HTTP, en este caso para Modificar un código de respuesta HTTP	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El código de respuesta HTTP debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Códigos de Respuesta HTTP*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del código de respuesta HTTP. 3. El usuario debe pinchar sobre el código de respuesta HTTP que quiere modificar y el sistema debe llevarlo a la vista de Adicionar código de respuesta HTTP, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar el código de respuesta HTTP 4. El usuario modifica el campo 'descripción 'en el formulario, este dato debe ser una cadena de caracteres y aceptar hasta 50 caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de os códigos de respuesta HTTP con el código de respuesta HTTP agregado al final de la lista y un mensaje diciendo que el código de respuesta HTTP fue modificado correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió el código de respuesta HTTP correctamente y se mantiene en el formulario para poder adicionar un nuevo código de respuesta HTTP c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió el código de respuesta HTTP correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar el código de respuesta HTTP d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados al código de respuesta HTTP que se quiere eliminar y da dos opciones (si quiere eliminar el código de respuesta HTTP, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 121 Prueba de Aceptación 36

Caso de prueba de aceptación	
Código: HU4_P4	**Historia de usuario:** 4
Nombre: Eliminar código de respuesta HTTP	
Descripción: Prueba para la funcionalidad Gestionar Código de respuesta HTTP, en este caso para eliminar un código de respuesta HTTP	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El código de respuesta HTTP debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Códigos de respuesta HTTP*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del código de respuesta HTTP. 3. El usuario selecciona el código de respuesta HTTP que quiere eliminar marcando el cuadro que aparece delante del identificador, busca la acción eliminar código de respuesta HTTP seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados al código de respuesta HTTP y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina el código de respuesta HTTP con todos los elementos asociados a él y muestra el mensaje se eliminó 1 código de respuesta HTTP satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de los códigos de respuestas HTTP	
Evaluación de la prueba: Satisfactoria	

Tabla 122 Prueba de Aceptación 37

Caso de prueba de aceptación	
Código: HU4_P5	**Historia de usuario:** 4
Nombre: Buscar código de respuesta HTTP	
Descripción: Prueba para la funcionalidad Gestionar Código de Respuesta HTTP, en este caso para Buscar un código de respuesta HTTP	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El código de respuesta HTTP debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Códigos de respuesta HTTP*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del código de respuesta HTTP. 3. El usuario escribe la descripción del código de respuesta que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con el código de respuesta seleccionado, en caso de no encontrarse debe mostrar el mensaje de que el código de respuesta no fue encontrado	
Evaluación de la prueba: Satisfactoria	

Tabla 123 Prueba de Aceptación 38

Caso de prueba de aceptación	
Código: HU5_P1	**Historia de usuario:** 5
Nombre: Adicionar un agente de usuario	
Descripción: Prueba para la funcionalidad Gestionar Agente de usuario, en este caso para Adicionar agente de usuario (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El agente de usuario no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Agentes de usuario*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos del agente de usuario. 3. El usuario selecciona dentro de la vista el botón '*Anadir Agente de usuario*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del agente de usuario 4. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 50 y selecciona cualquiera de los tres botones que aparecen en el formulario: a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de agentes de usuario con el agente de usuario agregado al final de la lista b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó el agente de usuario correctamente y se mantiene en el formulario para poder adicionar un nuevo agente de usuario c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó el agente de usuario correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar el agente de usuario	
Evaluación de la prueba: Satisfactoria	

Tabla 124 Prueba de Aceptación 39

Caso de prueba de aceptación	
Código: HU5_P2	**Historia de usuario:** 5
Nombre: Adicionar un Agente de usuario	
Descripción: Prueba para la funcionalidad Gestionar Agente de usuario, en este caso para Adicionar agente de usuario (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El agente de usuario no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Agentes de usuario*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de un agente de usuario. 3. El usuario selecciona dentro de la vista el botón '*Anadir Agente de usuario*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del agente de usuario 4. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de un agente de usuario que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 5. El sistema muestra mensajes de error de ya existe un agente de usuario con ese nombre o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 125 Prueba de Aceptación 40

Caso de prueba de aceptación	
Código: HU5_P3	**Historia de usuario:** 5
Nombre: Modificar un agente de usuario	
Descripción: Prueba para la funcionalidad Gestionar Agente de usuario, en este caso para Modificar un agente de usuario	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El agente de usuario debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Agentes de usuario*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del agente de usuario. 3. El usuario debe pinchar sobre la descripción del agente de usuario que quiere modificar y el sistema debe llevarlo a la vista de Adicionar Agente de usuario, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar el Agente de usuario 4. El usuario modifica el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 50 y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de agentes de usuario con el agente de usuario agregado al final de la lista y un mensaje diciendo que el agente de usuario fue modificado correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió el agente de usuario correctamente y se mantiene en el formulario para poder adicionar un nuevo agente de usuario c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió el agente de usuario correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar el agente de usuario d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados al agente de usuario que se quiere eliminar y da dos opciones (si quiere eliminar el Agente de usuario, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 126 Prueba de Aceptación 41

Caso de prueba de aceptación	
Código: HU5_P4	**Historia de usuario:** 6
Nombre: Eliminar Agente de Usuario	
Descripción: Prueba para la funcionalidad Gestionar Referencia, en este caso para eliminar un Agente de usuario	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El agente de usuario debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción 'Agentes de Usuarios' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del agente de usuario. 3. El usuario selecciona el agente de usuario que quiere eliminar marcando el cuadro que aparece delante del identificador, busca la acción eliminar agente de usuario seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados al agente de usuario y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina el agente de usuario con todos los elementos asociados a él y muestra el mensaje se eliminó 1 Agente de Usuario satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de los agentes de usuarios	
Evaluación de la prueba: Satisfactoria	

Tabla 127 Prueba de Aceptación 42

Caso de prueba de aceptación	
Código: HU5_P5	**Historia de usuario:** 5
Nombre: Buscar agente de usuario	
Descripción: Prueba para la funcionalidad Gestionar Agente de usuario, en este caso para Buscar un agente de usuario	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El agente de usuario debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Agentes de usuario*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del agente de usuario. 3. El usuario escribe el nombre del país que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con el agente de usuario seleccionado, en caso de no encontrarse debe mostrar el mensaje de que el agente de usuario no fue encontrado	
Evaluación de la prueba: Satisfactoria	

Tabla 128 Prueba de Aceptación 43

Caso de prueba de aceptación	
Código: HU6_P1	**Historia de usuario:** 6
Nombre: Adicionar una referencia	
Descripción: Prueba para la funcionalidad Gestionar Referencia, en este caso para Adicionar una referencia (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La referencia no debe verse adicionado anteriormente	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Referencias*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la referencia. 3. El usuario selecciona dentro de la vista el botón '*Anadir Referencia*, el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la referencia 4. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 50 y selecciona cualquiera de los tres botones que aparecen en el formulario: p. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de referencias con la referencia agregada al final de la lista q. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó la referencia correctamente y se mantiene en el formulario para poder adicionar una nueva referencia r. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó la referencia correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la referencia	
Evaluación de la prueba: Satisfactoria	

Tabla 129 Prueba de Aceptación 44

Caso de prueba de aceptación	
Código: HU6_P2	**Historia de usuario:** 6
Nombre: Adicionar referencia	
Descripción: Prueba para la funcionalidad Gestionar Referencia, en este caso para Adicionar referencia (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La referencia no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Referencias*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la referencia. 3. El usuario selecciona dentro de la vista el botón '*Anadir Referencia*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la referencia 4. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de una referencia que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 5. El sistema muestra mensajes de error de ya existe una referencia con esa descripción o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 130 Prueba de Aceptación 45

Caso de prueba de aceptación	
Código: HU6_P4	**Historia de usuario:** 6
Nombre: Eliminar referencia	
Descripción: Prueba para la funcionalidad Gestionar Referencia, en este caso para eliminar una referencia	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La referencia debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Referencias*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la referencia. 3. El usuario selecciona la referencia que quiere eliminar marcando el cuadro que aparece delante del identificador, busca la acción eliminar referencia seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados al referencia y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina la referencia con todos los elementos asociados a él y muestra el mensaje se eliminó 1 Referencia satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de las referencias	
Evaluación de la prueba: Satisfactoria	

Tabla 131 Prueba de Aceptación 46

Caso de prueba de aceptación	
Código: HU6_P5	**Historia de usuario:** 6
Nombre: Buscar referencia	
Descripción: Prueba para la funcionalidad Gestionar Referencia, en este caso para Buscar una referencia	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La referencia debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Petición'* 2. El usuario selecciona dentro de las opciones del módulo Petición la opción '*Referencias*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la referencia. 3. El usuario escribe la descripción de la referencia que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con la referencia seleccionado, en caso de no encontrarse debe mostrar el mensaje de que la referencia no fue encontrada	
Evaluación de la prueba: Satisfactoria	

Tabla 132 Prueba de Aceptación 47

Caso de prueba de aceptación	
Código: HU7_P1	**Historia de usuario:** 7
Nombre: Adicionar una URL	
Descripción: Prueba para la funcionalidad Gestionar URL, en este caso para Adicionar URL (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La URL no debe verse adicionado anteriormente.	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*URL*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de la URL. 3. El usuario selecciona dentro de la vista el botón '*Anadir URL*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la URL 4. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 70 y selecciona cualquiera de los tres botones que aparecen en el formulario: a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de URL con la URL agregada al final de la lista b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó la URL correctamente y se mantiene en el formulario para poder adicionar una nueva URL c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó la URL correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar la URL	
Evaluación de la prueba: Satisfactoria	

Tabla 133 Prueba de Aceptación 48

Caso de prueba de aceptación	
Código: HU7_P2	**Historia de usuario:** 7
Nombre: Adicionar un URL	
Descripción: Prueba para la funcionalidad Gestionar URL, en este caso para Adicionar URL (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La URL no debe verse adicionado anteriormente.	
Pasos de ejecución: 6. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 7. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*URL*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de una URL. 8. El usuario selecciona dentro de la vista el botón '*Anadir URL*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos de la URL 9. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de una URL que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 10. El sistema muestra mensajes de error de ya existe una URL con ese nombre o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 134 Prueba de Aceptación 49

Caso de prueba de aceptación	
Código: HU7_P3	**Historia de usuario:** 7
Nombre: Modificar un URL	
Descripción: Prueba para la funcionalidad Gestionar URL, en este caso para Modificar un URL	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La URL debe existir en el sistema	
Pasos de ejecución: 5. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 6. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*URL*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la URL. 7. El usuario debe pinchar sobre la descripción de la URL que quiere modificar y el sistema debe llevarlo a la vista de Adicionar URL, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar la URL 8. El usuario modifica el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 70 y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de URL con la URL agregada al final de la lista y un mensaje diciendo que la URL fue modificado correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió la URL correctamente y se mantiene en el formulario para poder adicionar una nueva URL c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió la URL correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar la URL d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados a la URL que se quiere eliminar y da dos opciones (si quiere eliminar la URL, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 135 Prueba de Aceptación 50

Caso de prueba de aceptación	
Código: HU7_P4	**Historia de usuario:** 7
Nombre: Eliminar una URL	
Descripción: Prueba para la funcionalidad Gestionar URL, en este caso para eliminar una URL	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La URL debe existir en el sistema	
Pasos de ejecución: 1. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción *'Incidente'* 2. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*URL*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la URL. 3. El usuario selecciona la URL que quiere eliminar marcando el cuadro que aparece delante del identificar, busca la acción eliminar URL seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados a la URL y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina la URL con todos los elementos asociados a él y muestra el mensaje se eliminó 1 URL satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de las URL	
Evaluación de la prueba: Satisfactoria	

Tabla 136 Prueba de Aceptación 51

Caso de prueba de aceptación	
Código: HU7_P5	**Historia de usuario:** 7
Nombre: Buscar URL	
Descripción: Prueba para la funcionalidad Gestionar URL, en este caso para Buscar una URL	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ La URL debe existir en el sistema	
Pasos de ejecución: 4. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Incidente'* 5. El usuario selecciona dentro de las opciones del módulo Incidente la opción '*URL*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos de la URL. 6. El usuario escribe el nombre del país que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con la URL seleccionada, en caso de no encontrarse debe mostrar el mensaje de que la URL no fue encontrada	
Evaluación de la prueba: Satisfactoria	

Tabla 137 Prueba de Aceptación 52

Caso de prueba de aceptación	
Código: HU13_P1	**Historia de usuario:** 13
Nombre: Adicionar un grupo	
Descripción: Prueba para la funcionalidad Gestionar grupo, en este caso para Adicionar grupo (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El grupo no debe verse adicionado anteriormente.	
Pasos de ejecución: 9. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Autenticación y Autorización'* 10. El usuario selecciona dentro de las opciones del módulo Autenticación y Autorización la opción 'Grupos' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos del grupo. 11. El usuario selecciona dentro de la vista el botón '*Anadir grupo*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del grupo 12. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 50 y selecciona cualquiera de los tres botones que aparecen en el formulario: a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de grupo con el grupo agregada al final de la lista b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó el grupo correctamente y se mantiene en el formulario para poder adicionar un nuevo grupo c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó el grupo correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar el grupo	
Evaluación de la prueba: Satisfactoria	

Tabla 138 Prueba de Aceptación 53

Caso de prueba de aceptación	
Código: HU13_P2	**Historia de usuario:** 13
Nombre: Adicionar un grupo	
Descripción: Prueba para la funcionalidad Gestionar grupo, en este caso para adicionar grupo (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El grupo no debe verse adicionado anteriormente.	
Pasos de ejecución: 11. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Autenticación y Autorización'* 12. El usuario selecciona dentro de las opciones del módulo Autenticación y Autorización la opción 'Grupos' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos de un grupo. 13. El usuario selecciona dentro de la vista el botón '*Anadir grupo*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del grupo 14. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de un grupo que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 15. El sistema muestra mensajes de error de ya existe un grupo con ese nombre o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 139 Prueba de Aceptación 54

Caso de prueba de aceptación	
Código: HU13_P3	**Historia de usuario:** 13
Nombre: Modificar un grupo	
Descripción: Prueba para la funcionalidad Gestionar grupo, en este caso para modificar un grupo	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El grupo debe existir en el sistema	
Pasos de ejecución: 9. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Autenticación y Autorización"* 10. El usuario selecciona dentro de las opciones del módulo Autenticación y Autorización la opción 'Grupos' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del grupo. 11. El usuario debe pinchar sobre la descripción del grupo que quiere modificar y el sistema debe llevarlo a la vista de adicionar grupo, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar el grupo 12. El usuario modifica el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 50 y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de grupo con el grupo agregada al final de la lista y un mensaje diciendo que el grupo fue modificado correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió el grupo correctamente y se mantiene en el formulario para poder adicionar un nuevo grupo c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió el grupo correctamente y puedes seguir modificándolo, se mantiene en el formulario para poder modificar el grupo d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados a el grupo que se quiere eliminar y da dos opciones (si quiere eliminar el grupo, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 140 Prueba de Aceptación 55

Caso de prueba de aceptación	
Código: HU13_P4	**Historia de usuario:** 13
Nombre: Eliminar un grupo	
Descripción: Prueba para la funcionalidad Gestionar grupo, en este caso para eliminar un grupo	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El grupo debe existir en el sistema	
Pasos de ejecución: 4. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción *'Autenticación y Autorización'* 5. El usuario selecciona dentro de las opciones del módulo Autenticación y Autorización la opción 'G*rupos*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del grupo. 6. El usuario selecciona el grupo que quiere eliminar marcando el cuadro que aparece delante del identificar, busca la acción eliminar grupo seleccionado en el cuadro de texto que se encuentra en la parte superior izquierda del panel de trabajo y se da la opción de ir, el sistema debe llevarlo a una vista donde aparecen todos los datos asociados al grupo y dos opciones posibles: a. El usuario selecciona la opción Sí, estoy seguro y el sistema elimina el grupo con todos los elementos asociados a él y muestra el mensaje se eliminó 1 grupo satisfactoriamente. b. El usuario selecciona la opción No, llévame atrás y el sistema lo regresa a la vista donde aparece la lista de las clasificaciones de grupo	
Evaluación de la prueba: Satisfactoria	

Tabla 141 Prueba de Aceptación 56

Caso de prueba de aceptación	
Código: HU13_P5	**Historia de usuario:** 13
Nombre: Buscar grupo	
Descripción: Prueba para la funcionalidad Gestionar grupo, en este caso para buscar un grupo	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El grupo debe existir en el sistema	
Pasos de ejecución: 7. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Autenticación y Autorización'* 8. El usuario selecciona dentro de las opciones del módulo Autenticación y Autorización la opción 'Grupos' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del grupo. 9. El usuario escribe el nombre del país que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con el grupo seleccionada, en caso de no encontrarse debe mostrar el mensaje de que el grupo no fue encontrada	
Evaluación de la prueba: Satisfactoria	

Tabla 142 Prueba de Aceptación 57

Caso de prueba de aceptación	
Código: HU14_P1	**Historia de usuario:** 14
Nombre: Adicionar un usuario	
Descripción: Prueba para la funcionalidad Gestionar Usuario, en este caso para Adicionar una usuaria (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El usuario no debe verse adicionado anteriormente	
Pasos de ejecución: 13. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción *'Autenticación y Autorización'* 14. El usuario selecciona dentro de las opciones del módulo Usuario la opción '*Usuarios*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos del usuario. 15. El usuario selecciona dentro de la vista el botón '*Anadir Usuario*, el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del usuario 16. El usuario completa el campo 'descripción 'en el formulario, este dato es una cadena de caracteres de longitud 132 y selecciona cualquiera de los tres botones que aparecen en el formulario: s. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de peticiones con el usuario agregada al final de la lista t. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se agregó el usuario correctamente y se mantiene en el formulario para poder adicionar un nuevo usuario u. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se agregó el usuario correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar el usuario	
Evaluación de la prueba: Satisfactoria	

Tabla 143 Prueba de Aceptación 58

Caso de prueba de aceptación	
Código: HU14_P2	**Historia de usuario:** 14
Nombre: Adicionar usuario	
Descripción: Prueba para la funcionalidad Gestionar Usuario, en este caso para Adicionar usuario (caso negativo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El usuario no debe verse adicionado anteriormente.	
Pasos de ejecución: 11. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Usuario'* 12. El usuario selecciona dentro de las opciones del módulo Usuario la opción '*Peticiones*' y el sistema debe mostrar en el panel derecho una vista que permite gestionar los datos del usuario. 13. El usuario selecciona dentro de la vista el botón '*Anadir Usuario*', el sistema debe llevarlo hasta otro formulario donde podrá entrar los datos del usuario 14. El usuario completa el campo 'descripción 'en el formulario introduciendo el nombre de un usuario que ya existe o un dato que no sea una cadena de caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario: 15. El sistema muestra mensajes de error de ya existe un usuario con esa descripción o que el dato que está entrando no es correcto	
Evaluación de la prueba: No Satisfactoria	

Tabla 144 Prueba de Aceptación 59

Caso de prueba de aceptación	
Código: HU14_P3	**Historia de usuario:** 14
Nombre: Modificar un usuario	
Descripción: Prueba para la funcionalidad Gestionar Usuario, en este caso para Modificar un usuario	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El usuario debe existir en el sistema	
Pasos de ejecución: 13. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Usuario'* 14. El usuario selecciona dentro de las opciones del módulo Usuario la opción '*Peticiones*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del usuario. 15. El usuario debe pinchar sobre el usuario que quiere modificar y el sistema debe llevarlo a la vista de Adicionar usuario, en la que se agrega la opción de eliminar en el caso que una de las modificaciones que quiera hacer sea eliminar el usuario 16. El usuario modifica el campo 'descripción 'en el formulario, este dato debe ser una cadena de caracteres y aceptar hasta 132 caracteres y selecciona cualquiera de los tres botones que aparecen en el formulario, o la opción eliminar. a. El usuario selecciona el botón 'Guardar 'y el sistema muestra la lista de os peticiones con el usuario agregado al final de la lista y un mensaje diciendo que el usuario fue modificado correctamente. b. El usuario selecciona el botón 'Guardar y añadir otro ', el sistema muestra el mensaje que se cambió el usuario correctamente y se mantiene en el formulario para poder adicionar un nuevo usuario c. El usuario selecciona el botón 'Guardar y continuar editando ', el sistema muestra el mensaje que se cambió el usuario correctamente y puedes seguir modificándola, se mantiene en el formulario para poder modificar el usuario d. El usuario selecciona la opción eliminar, el sistema debe mostrar una vista donde se muestran los datos asociados al usuario que se quiere eliminar y da dos opciones (si quiere eliminar el usuario, no llévame atrás)	
Evaluación de la prueba: Satisfactoria	

Tabla 145 Prueba de Aceptación 60

Caso de prueba de aceptación	
Código: HU14_P5	**Historia de usuario:** 14
Nombre: Buscar usuario	
Descripción: Prueba para la funcionalidad Gestionar Usuario, en este caso para Buscar un usuario	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ El usuario debe existir en el sistema	
Pasos de ejecución: 10. El usuario da clic en el menú lateral izquierdo para desplegar las opciones del módulo para ello debe dar clic en la opción '*Usuario'* 11. El usuario selecciona dentro de las opciones del módulo Usuario la opción '*Peticiones*' y debe mostrarse en el panel derecho una vista que permite gestionar los datos del usuario. 12. El usuario escribe la descripción del usuario que quiere buscar en el cuadro que aparece en la parte superior derecha de la vista de trabajo, el sistema debe mostrar la lista con el usuario seleccionado, en caso de no encontrarse debe mostrar el mensaje de que el usuario no fue encontrada	
Evaluación de la prueba: Satisfactoria	

Iteración 3

Tabla 146 Prueba de Aceptación 61

Caso de prueba de aceptación	
Código: HU18_P1	**Historia de usuario:** 18
Nombre: Buscar dirección IP.	
Descripción: Prueba para la funcionalidad Buscar número IP, en este caso para mostrar los datos asociados al número IP buscado. (caso positivo)	
Condiciones de ejecución: ➢ El usuario debe estar previamente autenticado en el sistema ➢ Debe existir el número IP en la base de datos	
Pasos de ejecución: 1. El usuario da clic en el cuadro de texto que aparece con una lupa que aparece en la parte superior izquierda del proyecto y escribe el número IP que quiere buscar en la base de datos 2. El sistema devuelve una vista con el resultado de la búsqueda, dónde se muestra, un mensaje que especifica la cantidad de peticiones que tiene ese número IP en la base de datos y muestra además los datos de las peticiones.	
Evaluación de la prueba: Satisfactoria	