

Universidad de las Ciencias Informáticas

Facultad 2



Sistema informático para la gestión de la autorización y control de dispositivos inalámbricos en la Universidad de las Ciencias Informáticas.

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

Autores:

Leandro Manuel Hernández Mira

Héctor Alonso Jiménez

Tutores:

MSc. Ramón Alexander Anglada Martínez

Ing. Yenlys Guerra Dávila

La Habana, 2016

“Año 58 de la Revolución”

DECLARACIÓN DE AUTORÍA

Declaramos ser autores de la presente tesis y reconocemos a la Universidad de las Ciencias Informáticas los derechos patrimoniales sobre ésta, con carácter exclusivo.

Para que así conste firmamos la presente a los _____ días del mes de _____ del año _____.

Leandro Manuel Hernández Mira

Autor

Héctor Alonso Jiménez

Autor

MSc. Ramón Alexander Anglada Martínez

Tutor

Ing. Yenlys Guerra Dávila

Tutor

RESUMEN

En la actualidad, son muchas las organizaciones que pretenden mantener un control sobre los dispositivos que acceden a su sistema de red. Esto contribuye a que se lleven a cabo procesos para autorizar el acceso de un dispositivo a un sistema de este tipo. La Universidad de las Ciencias Informáticas tiene definido un procedimiento para autorizar y controlar los dispositivos inalámbricos que acceden a la red inalámbrica. Este procedimiento conlleva al llenado de una planilla que contiene los datos de la persona que solicita la autorización y los datos del dispositivo que se desea autorizar. En la actualidad existe demora en el procesamiento de las solicitudes y además no se utiliza la información almacenada en la planilla de solicitud. La Universidad de las Ciencias Informáticas no cuenta con un software que gestione las solicitudes realizadas para llevar un control más eficiente de toda esta información.

La presente investigación está encaminada a darle solución a las limitantes señaladas anteriormente para lograr un mejor control en la gestión de la autorización de los dispositivos inalámbricos y disminuir el tiempo de procesamiento de las solicitudes.

Palabras claves: autorización, control, dispositivo inalámbrico, planilla, procedimiento.

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN	1
CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA	4
1.1 Introducción.....	4
1.2 Conceptos fundamentales asociados al dominio del problema.....	4
1.3 Sistemas similares.....	4
1.3.1 PacketFence	4
1.3.2 OpenNAC	4
1.3.3 Cisco Clean Access.....	5
1.3.4 Extreme Access Control	5
1.3.5 Conclusiones de las soluciones estudiadas.....	6
1.4 Metodología de desarrollo de software	6
1.5 Lenguajes, herramientas y tecnologías.....	7
1.5.1 Lenguajes de programación	7
1.5.2 Framework de desarrollo	8
1.5.3 Sistema Gestor de Base de Datos.....	8
1.6 Conclusiones del capítulo.....	9
CAPÍTULO 2: PROPUESTA DE SOLUCIÓN	10
2.1 Introducción.....	10
2.2 Análisis del procedimiento de autorización y control de dispositivos que acceden a la red inalámbrica en la Universidad de las Ciencias Informáticas	10
2.3 Propuesta de Sistema	10
2.4 Características no funcionales del sistema	11
2.5 Conclusiones del capítulo.....	12
CAPÍTULO 3: EXPLORACIÓN Y PLANIFICACIÓN	14
3.1 Introducción.....	14
3.2 Exploración.....	14
3.3 Planificación	20
3.4 Conclusiones del capítulo.....	22

CAPÍTULO 4: DISEÑO E IMPLEMENTACIÓN.....	23
4.1 Introducción.....	23
4.2 Diseño	23
4.2.1 Patrón Arquitectónico	23
4.2.1.1 Modelo Vista Controlador (MVC).....	24
4.2.2 Patrones de diseño.....	24
4.2.3 Tarjetas CRC.....	26
4.2.4 Modelo de Datos	33
4.3 Implementación	33
4.4 Conclusiones del capítulo.....	35
CAPÍTULO 5: VALIDACIÓN DE PROPUESTA	37
CONCLUSIONES GENERALES	54
RECOMENDACIONES	55
REFERENCIAS BIBLIOGRÁFICAS	56
BIBLIOGRAFÍA	58
ANEXOS	60

ÍNDICE DE FIGURAS

Figura 1: Propuesta de solución	11
Figura 2: Modelo-Vista-Controlador (tomado del libro Desarrollo web ágil con Symfony2)	24
Figura 3: Modelo de datos	33
Figura 4: Resultados obtenidos de las pruebas unitarias en 1era iteración.....	37
Figura 5: Resultados obtenidos de las pruebas unitarias en 2da iteración	38
Figura 6: Resultados obtenidos de las pruebas unitarias en 3era iteración.....	38
Figura 7: Fragmento de código de pruebas unitarias	39

ÍNDICE DE TABLAS

Tabla 1: Historia de Usuario - Procesar planillas de solicitud	15
Tabla 2: Historia de Usuario - Gestionar permisos de firma	16
Tabla 3: Historia de Usuario - Gestionar configuraciones	17
Tabla 4: Historia de Usuario - Gestionar los tipos de dispositivos permitidos	17
Tabla 5: Historia de Usuario - Gestionar fabricantes de tarjetas de red y sus MACs	18
Tabla 6: Historia de Usuario - Gestionar marcas y modelos de los dispositivos permitidos	19
Tabla 7: Historia de Usuario - Generar reportes	19
Tabla 8: Estimación de esfuerzo por Historias de Usuario	20
Tabla 9: Plan de duración de las iteraciones	22
Tabla 10: Plan de entregas	22
Tabla 11: Tarjeta CRC para la clase AreaController	26
Tabla 12: Tarjeta CRC para la clase ConfiguracionController	26
Tabla 13: Tarjeta CRC para la clase EstadisticasController	26
Tabla 14: Tarjeta CRC para la clase MacvendorsController	27
Tabla 15: Tarjeta CRC para la clase MarcaController	27
Tabla 16: Tarjeta CRC para la clase ModeloController	27
Tabla 17: Tarjeta CRC para la clase PDFController	27
Tabla 18: Tarjeta CRC para la clase PermisoController	28
Tabla 19: Tarjeta CRC para la clase PlanillaController	28
Tabla 20: Tarjeta CRC para la clase TipoDispositivosController	28
Tabla 21: Tarjeta CRC para la clase UsuarioController	28
Tabla 22: Tarjeta CRC para la clase MTArea	29
Tabla 23: Tarjeta CRC para la clase MTConfiguracion	29
Tabla 24: Tarjeta CRC para la clase MTMacVendors	29
Tabla 25: Tarjeta CRC para la clase MTMarca	29
Tabla 26: Tarjeta CRC para la clase MTModelo	30
Tabla 27: Tarjeta CRC para la clase MTPlanilla	30
Tabla 28: Tarjeta CRC para la clase MTTipoDispositivosPermitidos	30
Tabla 29: Tarjeta CRC para la clase MTUsuario	31
Tabla 30: Tarjeta CRC para la clase MTUsuario_Area	31
Tabla 31: Tarjeta CRC para la clase ConfiguracionRepository	31
Tabla 32: Tarjeta CRC para la clase MacvendorsRepository	32
Tabla 33: Tarjeta CRC para la clase MarcaRepository	32
Tabla 34: Tarjeta CRC para la clase ModeloRepository	32
Tabla 35: Tarjeta CRC para la clase PermisoRepository	32

Tabla 36: Tarjeta CRC para la clase PlanillaRepository	32
Tabla 37: Tarjeta CRC para la clase TiposDispositivosRepository	33
Tabla 38: Tarea de Ingeniería Solicitar planilla	34
Tabla 39: Tarea de Ingeniería Insertar permisos de firma	35
Tabla 40: Tarea de Ingeniería Mostrar configuración	35
Tabla 41: Prueba de aceptación: Listar planillas	40
Tabla 42: Prueba de aceptación: Solicitar planilla	40
Tabla 43: Prueba de aceptación: Cancelar planilla	41
Tabla 44: Prueba de aceptación: Ver planilla en formato pdf	41
Tabla 45: Prueba de aceptación: Firmar como directivo	42
Tabla 46: Prueba de aceptación: Mostrar permisos de firma	42
Tabla 47: Prueba de aceptación: Insertar permisos de firma	43
Tabla 48: Prueba de aceptación: Eliminar permisos de firma.....	43
Tabla 49: Prueba de aceptación: Mostrar configuración	44
Tabla 50: Prueba de aceptación: Modificar configuración	44
Tabla 51: Prueba de aceptación: Mostrar los tipos de dispositivos permitidos	45
Tabla 52: Prueba de aceptación: Modificar tipos de dispositivos permitidos	45
Tabla 53: Prueba de aceptación: Insertar tipos de dispositivos permitidos.....	46
Tabla 54: Prueba de aceptación: Eliminar tipos de dispositivos permitidos.....	46
Tabla 55: Prueba de aceptación: Comprobar validez de MAC	47
Tabla 56: Prueba de aceptación: Mostrar fabricantes de tarjetas de red.....	48
Tabla 57: Prueba de aceptación: Mostrar marcas.....	48
Tabla 58: Prueba de aceptación: Modificar Marcas	49
Tabla 59: Prueba de aceptación: Insertar marcas.....	49
Tabla 60: Prueba de aceptación: Eliminar marcas	50
Tabla 61: Prueba de aceptación: Mostrar modelos	50
Tabla 62: Prueba de aceptación: Modificar modelos.....	51
Tabla 63: Prueba de aceptación: Insertar modelos	51
Tabla 64: Prueba de aceptación: Eliminar modelos	52
Tabla 65: Prueba de aceptación: Mostrar reportes	52
Tabla 66: Tarea de ingeniería: Listar planillas.....	60
Tabla 67: Tarea de Ingeniería: Cancelar planilla.....	60
Tabla 68: Tarea de Ingeniería: Ver planillas en formato PDF.....	60
Tabla 69: Tarea de Ingeniería: Firmar como directivo	61
Tabla 70: Tarea de Ingeniería: Buscar información de planillas	61
Tabla 71: Tarea de Ingeniería: Exportar información	61
Tabla 72: Tarea de Ingeniería: Mostrar permisos de firma.....	62

Tabla 73: Tarea de Ingeniería Eliminar permisos de firma	62
Tabla 74: Tarea de Ingeniería: Modificar configuración.....	63
Tabla 75: Tarea de Ingeniería: Mostrar tipos de dispositivos permitidos	63
Tabla 76: Tarea de Ingeniería: Modificar tipos de dispositivos permitidos.....	63
Tabla 77: Tarea de Ingeniería: Insertar tipos de dispositivos permitidos	64
Tabla 78: Tarea de Ingeniería: Eliminar tipos de dispositivos permitidos	64
Tabla 79: Tarea de Ingeniería: Comprobar Validez de MAC	64
Tabla 80: Tarea de Ingeniería: Mostrar fabricantes de tarjetas de red y sus MACs	65
Tabla 81: Tarea de Ingeniería: Mostrar Marcas	65
Tabla 82: Tarea de Ingeniería: Modificar Marcas	65
Tabla 83: Tarea de Ingeniería: Insertar Marcas	66
Tabla 84: Tarea de Ingeniería: Eliminar Marcas.....	66
Tabla 85: Tarea de Ingeniería: Mostrar Modelos.....	66
Tabla 86: Tarea de Ingeniería: Modificar Modelos	67
Tabla 87: Tarea de Ingeniería: Insertar Modelos.....	67
Tabla 88: Tarea de Ingeniería: Eliminar Modelos.....	67
Tabla 89: Tarea de Ingeniería: Mostrar Reportes.....	68

INTRODUCCIÓN

El desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) en la actualidad ha generado una evolución en las diferentes esferas de la sociedad. Es por ello que varias empresas y organizaciones han extendido el uso de estas tecnologías para llevar a cabo sus actividades.

Las universidades han considerado este desarrollo una vía fundamental para ofrecer soporte a sus procesos puesto que garantiza la actualización del conocimiento más rápido, mejora su capacidad innovadora y eleva la calidad de sus servicios.

Actualmente, en la Universidad de las Ciencias Informáticas (UCI) se tiene definido un procedimiento para la autorización de dispositivos inalámbricos con el fin de garantizar el control sobre los medios que hacen uso del sistema de red inalámbrica.

La Universidad de las Ciencias Informáticas pretende convertirse en una universidad digital y para lograr su objetivo, dispone de valiosos recursos para el desarrollo de aplicaciones que permitan informatizar y mejorar la calidad de sus procesos. La Dirección de Seguridad Informática, área dentro de la universidad encargada de proteger la infraestructura y los datos contenidos en esta, ha desarrollado un sistema integrador de aplicaciones (Sistema de Gestión DSI) para lograr este objetivo. Uno de los procesos que no se encuentra incluido en este sistema es el procedimiento de autorización de dispositivos inalámbricos.

El procedimiento de autorización de dispositivos inalámbricos comienza cuando una persona solicita el registro de un medio tecnológico. Luego se le entrega una planilla para que este la complete con sus datos personales y los del dispositivo que desea autorizar. Después esta planilla debe ser firmada en primera instancia por el directivo del área, luego por un directivo del consejo universitario, después por el director de seguridad y protección y por último el director de seguridad informática. Una vez que la planilla es aprobada por estos cuatro directivos se escanea y se almacena como evidencia.

En la actualidad, el procedimiento de autorización de dispositivos inalámbricos presenta varios inconvenientes entre los que se refieren: las personas autorizadas a firmar las planillas no se encuentran en una misma ubicación dentro de la universidad lo cual provoca que exista demora en el proceso de aprobación debido a que la planilla se debe transportar a las áreas donde son firmadas; no existe un registro digital de las planillas autorizadas lo que conlleva a que no se puedan realizar búsquedas ni reportes sobre estas; además el usuario que realiza la solicitud no tiene conocimiento del estado en que se encuentra la planilla lo que provoca que se presente en varias ocasiones en el área de recogida.

Dada la problemática descrita se plantea el siguiente **problema** a resolver:

¿Cómo informatizar el procedimiento de autorización y control de dispositivos inalámbricos que acceden a la red inalámbrica en la Universidad de las Ciencias Informáticas?

El problema a resolver planteado, se enmarca en el **objeto de estudio**: el procedimiento de autorización y control de dispositivos inalámbricos que acceden a redes inalámbricas. Se traza como **objetivo general de la investigación**, desarrollar una aplicación que permita informatizar el procedimiento de autorización y control de dispositivos inalámbricos que acceden a la red inalámbrica en la Universidad de las Ciencias Informáticas. Se define como **campo de acción** el procedimiento de autorización y control de dispositivos inalámbricos que acceden a la red inalámbrica en la Universidad de las Ciencias Informáticas. Para dar cumplimiento al objetivo general se proponen las siguientes **tareas de la investigación**:

1. Estudio de sistemas existentes basados en la autorización y control de dispositivos que acceden a redes inalámbricas para analizar sus funcionalidades y características.
2. Estudio de las herramientas, metodologías y tecnologías necesarias para el desarrollo de la solución informática propuesta.
3. Análisis e identificación de funcionalidades para describir las características y restricciones que debe cumplir el sistema.
4. Estudio y análisis de los elementos correspondientes al diseño del software para guiar la implementación del mismo.
5. Estudio de los diferentes tipos de prueba para comprobar que la solución implementada cumple con los objetivos trazados.

Para el desarrollo de esta investigación y el logro de su objetivo, se utilizarán los siguientes **métodos de investigación científica**:

✓ **Métodos teóricos**

Analítico sintético: Se evidencia cuando se realiza un análisis de toda la teoría y documentación, que permiten la extracción de los elementos fundamentales relacionados con el proceso de autorización y control de dispositivos inalámbricos que acceden a redes inalámbricas.

Histórico-Lógico: Este método permite estudiar todo lo relacionado con los sistemas de autorización y control de dispositivos inalámbricos que acceden a redes inalámbricas, para así obtener un conocimiento histórico de su desarrollo y comportamiento.

✓ **Métodos Empíricos:**

Entrevista: Este método se utilizará para el desarrollo del sistema, detectando las necesidades del cliente a través del intercambio con él. Se realizan una serie de entrevistas con el cliente para identificar los principales problemas existentes y así poder satisfacer sus necesidades y obtener un software con la calidad requerida.

La presente investigación está organizada en cinco capítulos:

Capítulo 1. “**Fundamentación teórica**”.

Se hace referencia a los elementos teóricos que soportan la investigación, se presentan los lenguajes de programación y modelado así como las tecnologías y metodologías que se ajustan al desarrollo del trabajo.

Capítulo 2. “**Propuesta de Solución**”.

Se describe el flujo actual de los procesos a automatizar. Se detallan las funcionalidades y características que tendrá la propuesta del sistema, lo que posibilitará un mayor entendimiento del mismo.

Capítulo 3. “**Exploración y Planificación**”.

Se detallan las historias de usuario definidas, que recogen todas las funcionalidades a implementar. Se muestran además otros artefactos propios de la metodología de desarrollo, que se generan en estas etapas.

Capítulo 4. “**Diseño e Implementación**”.

Se hace referencia al diseño que tendrá el sistema a implementar y se muestra el desarrollo de la fase de implementación. Se realiza un acercamiento al patrón arquitectónico, a los patrones de diseño, a las Tarjetas CRC y finalmente se representa la estructura que tendrá la base de datos. También se realiza una descripción de las tareas de ingeniería por cada Historia de Usuario identificada.

Capítulo 5. “**Validación de la propuesta**”.

Se valida a través de pruebas de calidad propuestas por la metodología escogida, las funcionalidades del sistema construido. Se exponen los resultados obtenidos en las pruebas y se muestra la encuesta realizada a los usuarios del sistema para conocer el grado de adecuación de la herramienta al trabajo de los mismos.

CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA

1.1 Introducción

En el presente capítulo se describe la metodología, las tecnologías y los lenguajes utilizados para el desarrollo de la solución, así como un estudio del estado del arte del procedimiento de autorización y control de dispositivos inalámbricos que acceden a redes inalámbricas.

1.2 Conceptos fundamentales asociados al dominio del problema

Procedimiento: puede definirse como, todo aquel método implementado guiado por una serie de pasos ordenados en forma secuencial y plenamente clasificados según se necesite, para lograr un fin determinado o poder ejecutar algo en particular. Es un sistema donde se realizan un grupo de operaciones en sucesión, para lograr obtener un resultado para una situación dada (1).

Autorización: Se refiere a conceder o permitir a alguien el permiso o derecho para hacer determinada acción (2).

Control: Se refiere al proceso de comparar entre un rendimiento esperado y un rendimiento observado para verificar si se están cumpliendo los objetivos y tomar acciones correctivas cuando sea necesario (3).

Dispositivo inalámbrico: Son dispositivos que no necesitan estar conectados físicamente mediante cables. Se corresponden con una tecnología mediante la que todo dispositivo ofrece una conectividad vía ondas (4).

1.3 Sistemas similares

A partir del problema planteado se realizó un estudio de algunos sistemas que cubren el procedimiento de autorización de dispositivos con el objetivo de validar si se ajustan a las necesidades de la institución o evaluar los elementos positivos que cada uno pudiera aportar a la propuesta de solución.

1.3.1 PacketFence

PacketFence es un sistema para el control de acceso a la red que está basado en código abierto y gratuito. Esta solución permite a través de un sitio web autenticar y registrar dispositivos que solicitan acceso a la red, detectar anomalías en la red, aislar dispositivos problemáticos, controlar ancho de banda para cada dispositivo, etc. Está preparado para dar servicio tanto a redes pequeñas como a grandes redes heterogéneas donde conviven gran diversidad de dispositivos y puntos de accesos a la red. (5).

1.3.2 OpenNAC

OpenNAC es un sistema de código abierto para el control de acceso a redes LAN/WAN. Permite la autenticación, autorización y auditoría de todos los dispositivos conectados en la red. Aporta

soluciones como acceso a la red basada en políticas de acceso, posibilidad de notificar o poner en cuarentena a los usuarios, independientemente del dispositivo cliente, contabilidad y auditoría de acceso, entre otras (6).

Conclusiones sobre PacketFence y OpenNAC

A pesar de que estas soluciones son de código abierto y gratuito su utilización no es posible debido a que:

- ✓ PacketFence es un sistema que está desarrollado en el lenguaje de programación Perl y el Sistema de Gestión DSI utiliza el framework de desarrollo Symfony que hace uso del lenguaje PHP.
- ✓ OpenNAC está desarrollado en PHP pero no hace uso de algún framework de desarrollo que implemente el patrón arquitectónico Modelo-Vista-Controlador que es implementado por Symfony. Por lo que primero habría que analizar la infraestructura que ha sido diseñada por ellos para luego entender el flujo, después entender el código, adaptarlo al Modelo-Vista-Controlador y por último intentar integrarlo al Sistema de Gestión DSI. Todo esto sería un proceso trabajoso y se llevaría más tiempo que realizar una nueva solución.

1.3.3 Cisco Clean Access

Cisco Clean Access es un sistema para el control de acceso a redes que trabaja con un agente que recopila los datos en el dispositivo y un gestor para administrar las políticas. Es recomendable para redes homogéneas con dispositivos Cisco ya que no presentaría problemas de incompatibilidad (7).

Con Cisco Clean Access se puede:

- ✓ Reconocer a los usuarios, sus dispositivos y sus roles en la red.
- ✓ Evaluar si las máquinas son compatibles con las políticas de seguridad.
- ✓ Aplicar políticas de seguridad mediante el bloqueo, aislamiento y reparación de las máquinas que no cumplen.
- ✓ Proporcionar un fácil y seguro acceso para invitados.
- ✓ Auditoría e informe de quien está en la red.

1.3.4 Extreme Access Control

Extreme Access Control es un sistema para el control de acceso a redes que permite a los usuarios registrar sus propios dispositivos de forma automática utilizando sus credenciales. Proporciona una funcionalidad de identificación de usuario incluyendo la búsqueda, autenticación y control de acceso basado en roles. Permite una fácil integración con herramientas de gestión de redes, respuesta a las amenazas, seguridad de la información, gestión de eventos y detección de intrusos (8).

Conclusiones sobre Cisco Clean Access y Extreme Access Control

Después de realizar un estudio de estas soluciones se identificaron que eran herramientas privativas lo que provoca imposibilidad de modificación del código fuente, dependencia total de la empresa propietaria y mayor costo de adquisición.

1.3.5 Conclusiones de las soluciones estudiadas

Tras analizar las soluciones similares existentes se concluye que estas no cumplen con las características deseadas. A pesar de que ofrecen una funcionalidad para el registro automático de dispositivos, su utilización no es posible para la gestión de la autorización y control de dispositivos inalámbricos en la Universidad de las Ciencias Informáticas ya que no garantizan la continuidad del proceso de aprobación de planillas que se desarrolla en esta, pues este proceso es único y muy específico de este entorno. Además no se gestiona la misma información que se maneja en el registro de medios tecnológicos desarrollado en la Universidad de las Ciencias Informáticas.

1.4 Metodología de desarrollo de software

Las metodologías de desarrollo de software son un conjunto de procedimientos, técnicas y ayudas a la documentación para el desarrollo de productos de software (9).

Dentro de las metodologías de desarrollo de software existen dos grandes grupos: las metodologías tradicionales o robustas y las metodologías ágiles o ligeras. Las primeras se enfatizan en el uso exhaustivo de documentación durante todo el ciclo de vida del proyecto, se centran especialmente en el control del proceso, estableciendo rigurosamente las actividades involucradas, los artefactos que se deben producir y las herramientas y notaciones que se usarán. Además, estas metodologías son recomendadas para proyectos con grandes equipos de desarrollo. Por otra parte las metodologías ágiles están orientadas a proyectos pequeños con requisitos muy cambiantes donde se exige reducir drásticamente los tiempos de desarrollo pero manteniendo una alta calidad. También dan mayor valor al individuo, a la colaboración entre el cliente y el equipo de desarrollo y al desarrollo incremental del software con iteraciones muy cortas.

Entre las principales metodologías que guían el desarrollo de un software se encuentran las metodologías ágiles Programación Extrema (XP), SCRUM y Desarrollo Basado en Funcionalidades (FDD por sus siglas en inglés Feature Driven Development) y las tradicionales Proceso Unificado de Desarrollo (RUP) y Microsoft Solution Framework.

Una vez analizado esto se selecciona XP para el desarrollo del presente trabajo debido a que se adapta al desarrollo de proyectos pequeños y grandes, optimiza el tiempo de desarrollo, permite realizar el desarrollo del sistema en parejas para complementar los conocimientos, se basa en la retroalimentación continua entre el cliente y el equipo de desarrollo y se define especialmente para proyectos con funcionalidades imprecisas y muy cambiantes. Además para el desarrollo del presente trabajo se cuenta con un equipo de dos personas, un tiempo de desarrollo relativamente corto y los requisitos pueden cambiar a medida que avance el trabajo.

1.5 Lenguajes, herramientas y tecnologías

Para dar solución a la problemática, el módulo se desarrollará utilizando los lenguajes, herramientas y tecnologías definidas por la Dirección de Seguridad Informática (DSI) de manera que asegure satisfactoriamente la inclusión de la solución dentro del Sistema de Gestión DSI y pueda compartir y reutilizar todos los elementos que este sistema pone a disposición de sus módulos. Dentro del ambiente de desarrollo definido por la DSI se encuentran lenguajes de programación como PHP 5.3.4, CSS3, JavaScript, HTML5 y el lenguaje de plantillas Twig. Como framework de desarrollo del lado del servidor se tiene definido Symfony 2.7 y del lado del cliente Dojo en su versión 1.10. Como sistema gestor de base de datos se hace uso de la versión 9.2 de PostgreSQL. A continuación se explican algunas características de estas tecnologías para un mejor entendimiento.

1.5.1 Lenguajes de programación

1.5.1.1 PHP 5.3.4

PHP es un lenguaje de programación multiplataforma completamente orientado al desarrollo de aplicaciones web dinámicas con acceso a información almacenada en una Base de Datos. Posee una capacidad de conexión con la mayoría de los motores de base de datos que se utilizan en la actualidad, destaca su conectividad con MySQL y PostgreSQL. Es un lenguaje totalmente libre y de código abierto (10).

1.5.1.2 Hojas de Estilo en Cascadas (CSS3)

CSS es un mecanismo simple que describe cómo se va a mostrar un documento en la pantalla, o cómo se va a imprimir, o incluso cómo va a ser pronunciada la información presente en ese documento a través de un dispositivo de lectura. Esta forma de descripción de estilos ofrece a los desarrolladores el control total sobre estilo y formato de sus documentos. CSS se utiliza para dar estilo a documentos HTML y XML, separando el contenido de la presentación (11).

1.5.1.3 JavaScript (JS)

JS es un lenguaje ligero e interpretado, orientado a objetos, más conocido como el lenguaje de script para páginas web. Es un lenguaje script multi-paradigma, basado en prototipos, dinámico, soporta estilos de programación funcional, orientada a objetos e imperativa. Su código puede ser embebido en un documento HTML y se puede manipular dinámicamente su contenido (12). Se usa para manejar los datos del lado del cliente ya que permite dar respuestas a eventos iniciados por el usuario.

1.5.1.4 HTML5

HTML es el lenguaje de marcado predominante para la construcción de páginas web. Es un lenguaje de marcado descriptivo que se escribe en forma de etiquetas para definir la estructura de una página web y su contenido como texto, imágenes, entre otros, de modo que HTML es el encargado de describir (hasta cierto punto) la apariencia que tendrá la página web (13).

1.5.1.5 Twig

Twig es un motor de plantillas desarrollado para el lenguaje de programación PHP. Su objetivo es facilitar a los desarrolladores de aplicaciones web que utilizan la arquitectura MVC el trabajo con la parte de las vistas, gracias a que se trata de un sistema que resulta muy sencillo de aprender y capaz de generar plantillas con un código preciso y fácil de leer (14).

1.5.2 Framework de desarrollo

1.5.2.1 Symfony 2.7

Symfony es un proyecto PHP de software libre que permite crear aplicaciones y sitios web rápidos y seguros de forma profesional. Su código, y el de todos los componentes y librerías que incluye, se publican bajo la licencia MIT de **software libre**. Separa la lógica de negocio, la lógica de servidor y la presentación de la aplicación web. Proporciona varias herramientas y clases encaminadas a reducir el tiempo de desarrollo de una aplicación web compleja. Además, automatiza las tareas más comunes, permitiendo al desarrollador dedicarse por completo a los aspectos específicos de cada aplicación (15).

Symfony se diseñó para que fuera independiente del sistema gestor de bases de datos; siguiera la mayoría de mejores prácticas y patrones de diseño para la web; su código fuera fácil de leer; fácil de extender para permitir su integración con librerías desarrolladas por terceros y se pudiera ejecutar tanto en plataformas *nix (Unix, Linux, etc) como en plataformas Windows.

1.5.2.2 Dojo

Dojo es una herramienta open source DHTML (Dynamic HTML) destinado a facilitar el rápido desarrollo de JavaScript o de las aplicaciones basadas en Ajax y sitios web. Su idea es la de abstraer al desarrollador de las complejidades del DHTML y de las discrepancias existentes entre navegadores. Dojo provee gran cantidad de funcionalidades las cuales se dividen en tres grandes proyectos, Dojo Core, Dijit y DojoX. Dijit y DojoX están basadas en la sólida base que Dojo Core brinda. Dijit incorpora un conjunto de widgets con los cuales se pueden crear amigables interfaces en muy poco tiempo y escribiendo casi o ningún código JavaScript. DojoX es donde se desarrollan extensiones para Dojo Toolkit, sirve de cuna para nuevas ideas y pruebas de funcionalidades adicionales para el Toolkit principal (16).

1.5.3 Sistema Gestor de Base de Datos

1.5.3.1 PostgreSQL 9.2

PostgreSQL es un sistema de gestión de bases de datos objeto-relacional, distribuido bajo licencia BSD y con su código fuente disponible libremente. Es uno de los sistemas de gestión de bases de datos de código abierto más utilizados en el mercado (17).

Algunas de sus principales características son:

- ✓ **Alta concurrencia.** Mediante un sistema denominado MVCC (Acceso concurrente multiversión) PostgreSQL permite que mientras un proceso escribe en una tabla, otros accedan a la misma tabla sin necesidad de bloqueos. Cada usuario obtiene una visión consistente de lo último a lo que se le hizo commit. Esta estrategia es superior al uso de bloqueos por tabla o por filas común en otras bases, eliminando la necesidad del uso de bloqueos explícitos.
- ✓ **Multiplataforma y variadas herramientas de diseño y administración.** Existen instaladores de los servidores y clientes PostgreSQL para los sistemas operativos Windows y las distribuciones de Linux. También se dispone de diversas herramientas gráficas de alta calidad para el diseño: Toad, Data Architect, etc.
- ✓ **Diseñado para ambientes de alto volumen.** Al igual que los principales proveedores de SBD comerciales, PostgreSQL usa una estrategia de almacenamiento de filas llamada MVCC para conseguir una mucha mejor respuesta en ambientes de grandes volúmenes.

1.6 Conclusiones del capítulo

En este capítulo se realizó un resumen de los principales conceptos asociados al dominio del problema con el objetivo de lograr un mayor entendimiento del mismo. Se realizó un análisis de algunos de los sistemas similares que permitió identificar características y funcionalidades que pueden ser útiles para el desarrollo y el diseño del presente sistema. Además, se analizó y se seleccionó la metodología de desarrollo de software, las herramientas y tecnologías más adecuadas que permitirán obtener una aplicación robusta y que satisfaga plenamente las necesidades del cliente.

CAPÍTULO 2: PROPUESTA DE SOLUCIÓN

2.1 Introducción

En el presente capítulo se hace un análisis de los procesos del negocio que se desean informatizar, lo cual posibilita que se tenga un mayor conocimiento del mismo, en vista de lograr un sistema que cumpla con las necesidades reales del cliente. Además se describen las principales características del sistema que fundamenta esta investigación.

2.2 Análisis del procedimiento de autorización y control de dispositivos que acceden a la red inalámbrica en la Universidad de las Ciencias Informáticas

En la actualidad el procedimiento de autorización y control de dispositivos inalámbricos se realiza de forma manual. Una vez que el usuario completa la planilla con sus datos personales y los del dispositivo que desea autorizar, debe esperar la autorización del directivo de área, del directivo del consejo universitario, del director de seguridad y protección y por último la del director de seguridad informática. Estas personas no se encuentran en una misma ubicación dentro de la universidad y existe una persona encargada de entregar la planilla para que cada una de estas personas la firme. Una vez que la planilla es aprobada por los cuatro directivos esta se escanea y se almacena como evidencia de la realización de una solicitud. La planilla después que es aprobada tiene validez durante un curso escolar y una vez que se vence este período el usuario debe volver a realizar una solicitud.

2.3 Propuesta de Sistema

Como propuesta de solución que fundamenta esta investigación se plantea la creación de una aplicación web a la cual se podrá acceder mediante un sistema de autenticación que comprobará las credenciales del usuario a través de un servicio web. El módulo mostrará a los usuarios los datos de sus solicitudes y el estado en que se encuentran (pendiente, rechazada o aprobada). Además le dará opciones de solicitar una nueva planilla o cancelar alguna. Para solicitar alguna planilla el usuario deberá proporcionarle al sistema la marca, el modelo, el tipo de dispositivo que desea autorizar, así como la MAC de la tarjeta inalámbrica y el número de serie.

Luego de haber solicitado el registro de un medio tecnológico el sistema verificará si la MAC de la tarjeta inalámbrica es válida. Para comprobar la validez de una MAC el sistema deberá comprobar en la dirección <http://api.macvendors.com/> si existe dicha MAC. Si la MAC no se encuentra en la API la planilla queda en un estado pendiente y ningún directivo puede proceder con el proceso de aprobación. Después que se verifica que la MAC es válida, el sistema deberá permitir a los usuarios que tengan permiso de firma, aprobar o rechazar estas solicitudes. Para que una planilla se encuentre en el estado de aprobada el directivo del área, el directivo del consejo universitario, el director de seguridad y protección y el director de seguridad informática deberán haber aprobado la planilla. El proceso de aprobación deberá realizarse en ese orden.

El administrador tendrá acceso a gestionar (insertar, modificar, eliminar) los tipos de dispositivos que pueden ser autorizados, así como las marcas y los modelos asociados a estos tipos de dispositivos. Podrá definir la cantidad de dispositivos a la que un usuario puede solicitarle el registro en el sistema y podrá definir la duración de validez de una planilla. Además tendrá acceso a todos los reportes que se brinden en el sistema. En la figura 1 se muestra la propuesta de solución descrita anteriormente para un mejor entendimiento.

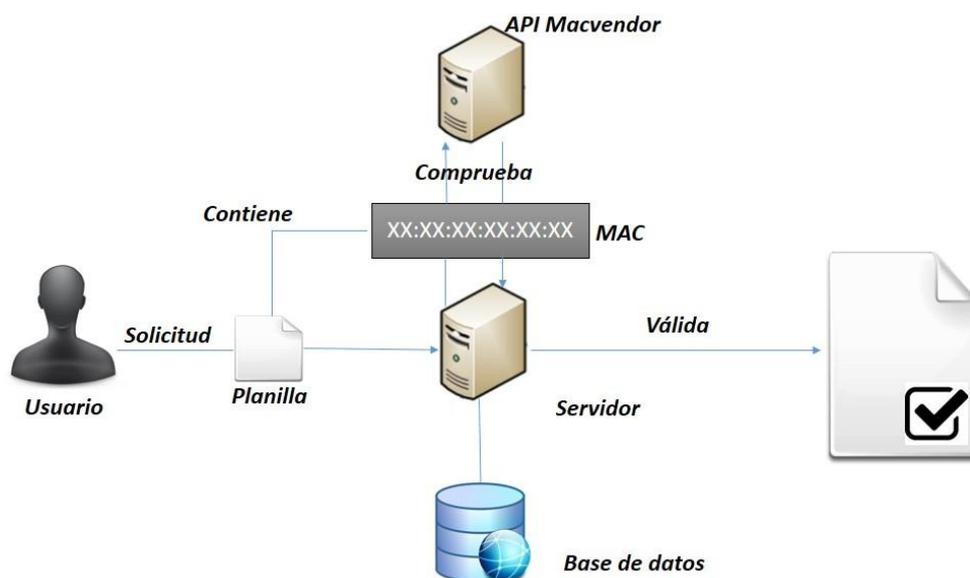


Figura 1: Propuesta de solución

2.4 Características no funcionales del sistema

Las características no funcionales son propiedades o cualidades que el producto debe tener. Debe pensarse en estas propiedades como las características que hacen al producto atractivo, usable, rápido o confiable.

Usabilidad

- ✓ Los elementos que conforman una interfaz de usuario, llámese imágenes, botones, campos de entrada de datos, deben tener un nombre sugerente, que logre que el usuario perciba la acción, además de mostrar una breve descripción de su función en la propia interfaz o con solo pasarle el cursor por encima.
- ✓ En el caso de los formularios deben especificar las reglas de sus campos, como pueden ser: los obligatorios, aquellos que solo aceptan tipos de datos específicos o longitudes de cadenas limitadas.

- ✓ Se debe garantizar que los contenidos tengan validez gramatical y correcta ortografía.
- ✓ El sistema debe contar con un estilo de presentación coherente para cada página.
- ✓ El sistema debe presentar una interfaz amigable que permita la fácil interacción con el mismo y llegar de manera rápida y efectiva a la información buscada. Debe, además, ser una interfaz de manejo cómodo que posibilite a los usuarios sin experiencia una rápida adaptación.

Software

En el cliente, aunque solo precisa de un navegador web, es necesario tener en consideración cuáles son adecuados y recomendables para hacer uso del sistema:

- ✓ Mozilla Firefox (versión 30 o superior).
- ✓ Internet Explorer (versión 6 o superior).
- ✓ Chrome (versión 20 o superior).

Hardware

Para el correcto funcionamiento del módulo se requiere para el servidor:

- ✓ PC Dual Core o superior.
- ✓ CPU 1.9 GHz o superior.
- ✓ 1 GB de RAM o superior.
- ✓ 160 GB de disco duro o superior.

Seguridad

- ✓ **Confidencialidad:** La información manejada por el sistema está protegida de acceso no autorizado y divulgación.
- ✓ **Integridad:** La información manejada por el sistema será objeto de cuidadosa protección contra la corrupción y estados inconsistentes, de la misma forma será considerada igual a la fuente o autoridad de los datos.
- ✓ **Disponibilidad:** Los usuarios autorizados se les garantizará el acceso a la información y que los dispositivos o mecanismos utilizados para lograr la seguridad no ocultarán o retrasarán a los usuarios para obtener los datos deseados en un momento dado.

2.5 Conclusiones del capítulo

En este capítulo se hizo un análisis del procedimiento de autorización y control de dispositivos que acceden a la red inalámbrica en la Universidad de las Ciencias Informáticas lo que permitió obtener una visión clara y concreta de las necesidades del cliente, las cuales se evidenciaron en la propuesta de solución y sentaron las bases para la construcción del sistema. Teniendo definidas las mismas ya se puede comenzar con la construcción de la propuesta de solución.

CAPÍTULO 3: EXPLORACIÓN Y PLANIFICACIÓN

3.1 Introducción

En el presente capítulo se hace referencia a las fases de Exploración y Planificación del proyecto de software que presenta esta investigación, propias de la metodología XP, bajo la cual se desarrolla. Se detallan además los artefactos obtenidos en dichas etapas del desarrollo.

3.2 Exploración

En esta fase, los clientes plantean a grandes rasgos las historias de usuario que son de interés para la primera entrega del producto. Al mismo tiempo el equipo de desarrollo se familiariza con las herramientas, tecnologías y prácticas que se utilizarán en el proyecto. Se prueba la tecnología y se exploran las posibilidades de la arquitectura del sistema construyendo un prototipo. La fase de exploración toma de pocas semanas a pocos meses, dependiendo del tamaño y familiaridad que tengan los programadores con la tecnología (18).

3.2.1 Historias de Usuario

Entre los artefactos que define la metodología seleccionada se encuentran las historias de usuario que son descripciones cortas y simples de las funcionalidades del sistema, narradas desde la perspectiva de la persona que desea dicha funcionalidad, usualmente un usuario. Son escritas a lo largo de todo el proyecto de desarrollo (19).

A continuación se detallan las historias de usuario identificadas durante la fase de Exploración del proyecto, que abarcan las funcionalidades del sistema propuesto.

- ✓ Procesar planillas de solicitud.
- ✓ Gestionar permisos de firma.
- ✓ Gestionar configuraciones.
- ✓ Gestionar los tipos de dispositivos permitidos.
- ✓ Gestionar fabricantes de tarjetas de red y sus MACs.
- ✓ Gestionar marcas y modelos de los dispositivos permitidos.
- ✓ Generar Reportes.

Historia de Usuario	
Número: 1	Nombre: Procesar planillas de solicitud
Prioridad: Alta	Riesgo en desarrollo: Alto
Iteración asignada: 1	Puntos estimados: 3

Descripción: El sistema debe permitir a un usuario poder realizar una solicitud, poder cancelarla y ver el estado en que se encuentra su planilla. Debe permitirle al usuario que tenga permisos poder comprobar si la MAC de la tarjeta inalámbrica introducida por el usuario es válida, debe permitir a los usuarios que tengan permiso poder aprobar o denegar una planilla y debe permitir descargar la planilla en formato pdf.

Observaciones: El usuario debe estar previamente autenticado en el sistema.

Prototipo de Interfaz:

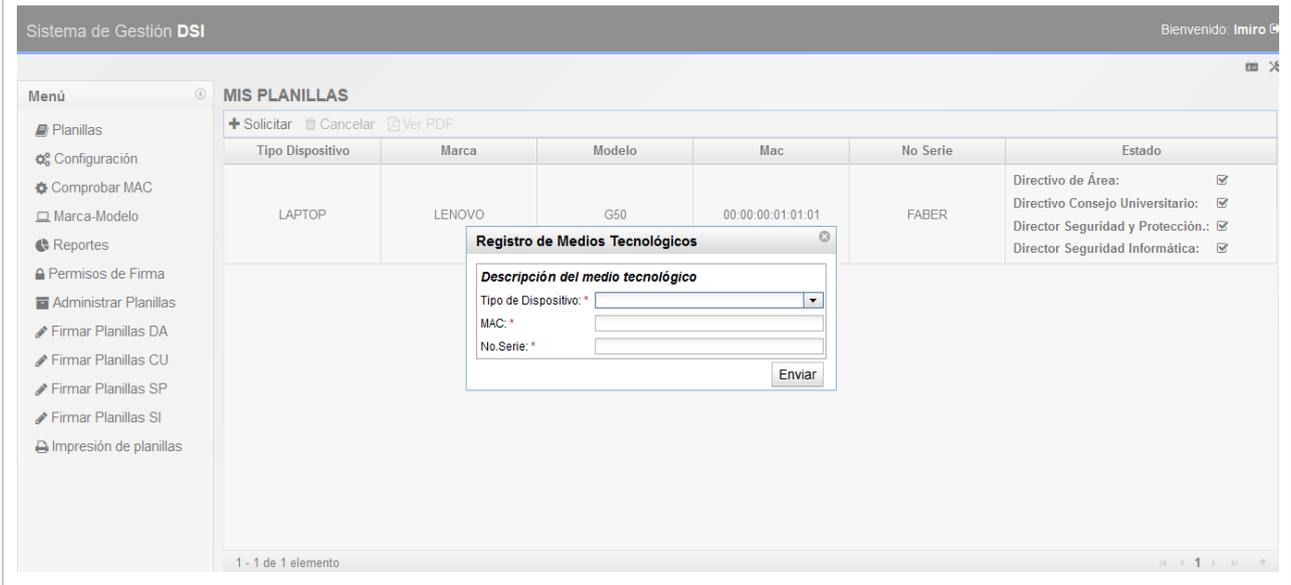


Tabla 1: Historia de Usuario - Procesar planillas de solicitud

Historia de Usuario	
Número: 2	Nombre: Gestionar permisos de firmas
Prioridad: Media	Riesgo en desarrollo: Alto
Iteración asignada: 2	Puntos estimados: 2
Descripción: El sistema debe permitirle al usuario que tenga permiso poder listar, insertar o eliminar los permisos de firma.	
Observaciones: El usuario debe estar previamente autenticado en el sistema.	
Prototipo de Interfaz:	

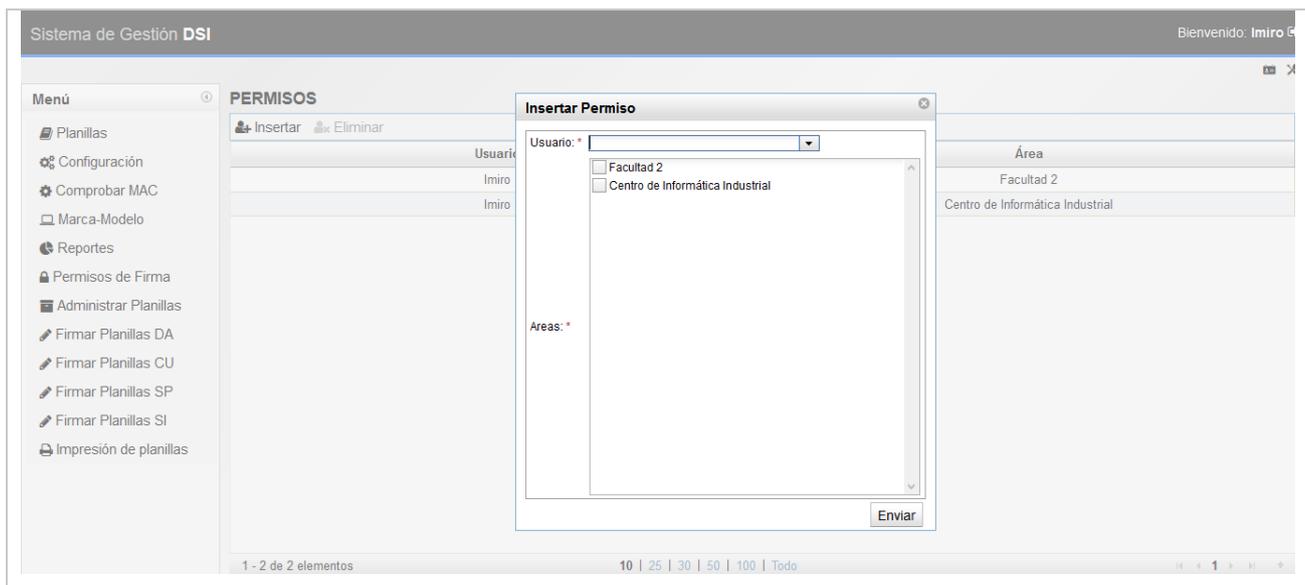


Tabla 2: Historia de Usuario - Gestionar permisos de firma

Historia de Usuario	
Número: 3	Nombre: Gestionar Configuraciones
Prioridad: Baja	Riesgo en desarrollo: Medio
Iteración asignada: 3	Puntos estimados: 0.2
Descripción: El sistema debe permitirle al usuario que tenga permiso poder modificar la cantidad de dispositivos permitidos por persona y la duración de validez de una planilla.	
Observaciones: Al comienzo del despliegue de la aplicación los valores por defecto que debe cargar el sistema deben ser de 1 curso de duración para la validez de una planilla y de 1 dispositivo permitido por persona. El usuario debe estar previamente autenticado en el sistema.	
Prototipo de Interfaz:	

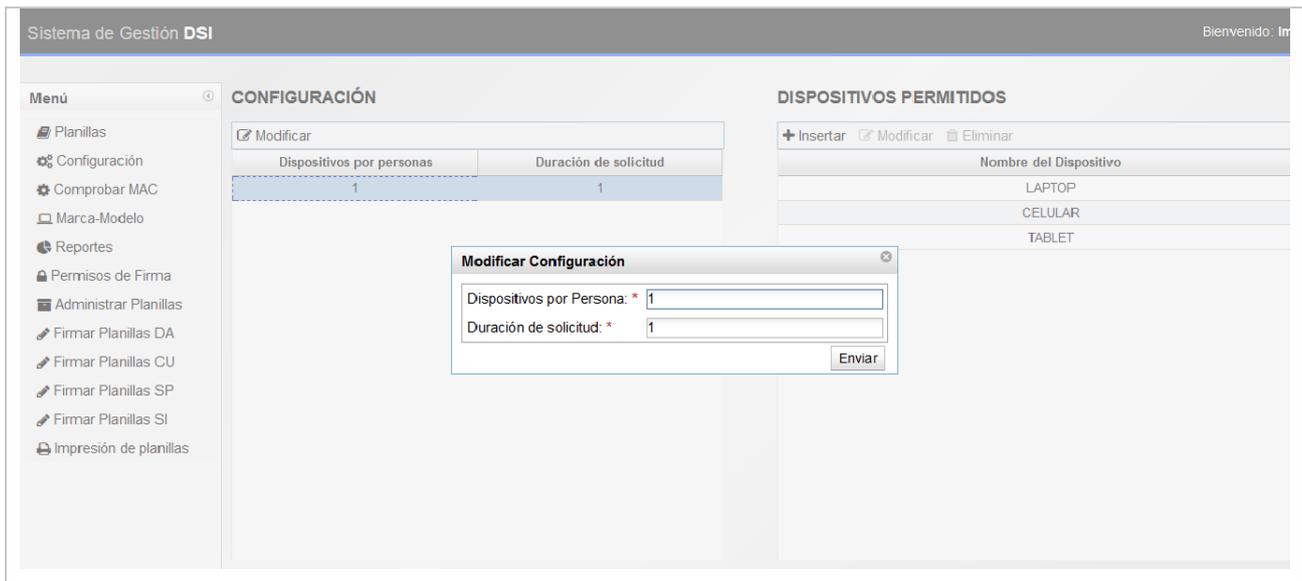


Tabla 3: Historia de Usuario - Gestionar configuraciones

Historia de Usuario	
Número: 4	Nombre: Gestionar los tipos de dispositivos permitidos
Prioridad: Baja	Riesgo en desarrollo: Medio
Iteración asignada: 3	Puntos estimados: 0.4
Descripción: El sistema debe permitirle al usuario que tenga permiso poder listar, insertar, modificar y eliminar los tipos de dispositivos permitidos, dígame laptops, celulares, tablets, etc.	
Observaciones: El usuario deberá estar previamente autenticado en el sistema.	
Prototipo de Interfaz:	

Tabla 4: Historia de Usuario - Gestionar los tipos de dispositivos permitidos

Historia de Usuario																																					
Número: 5	Nombre: Gestionar fabricantes de tarjetas de red y sus MACs																																				
Prioridad: Baja	Riesgo en desarrollo: Medio																																				
Iteración asignada: 3	Puntos estimados: 0.6																																				
Descripción: El sistema debe permitirle usuario que tenga permiso poder listar los fabricantes y sus MACs asignadas.																																					
Observaciones: El usuario debe estar previamente autenticado. Se deben realizar las acciones necesarias para que el sistema cargue un conjunto de datos desde la dirección http://www.bgplookingglass.com/mac-address-vendor-lookup .																																					
Prototipo de Interfaz:																																					
<table border="1"> <caption>MAC-FABRICANTES</caption> <thead> <tr> <th>MAC</th> <th>Fabricante</th> </tr> </thead> <tbody> <tr><td>00:00:00</td><td>XEROX CORPORATION</td></tr> <tr><td>00:00:01</td><td>XEROX CORPORATION</td></tr> <tr><td>00:00:02</td><td>XEROX CORPORATION</td></tr> <tr><td>00:00:03</td><td>XEROX CORPORATION</td></tr> <tr><td>00:00:04</td><td>XEROX CORPORATION</td></tr> <tr><td>00:00:05</td><td>XEROX CORPORATION</td></tr> <tr><td>00:00:06</td><td>XEROX CORPORATION</td></tr> <tr><td>00:00:07</td><td>XEROX CORPORATION</td></tr> <tr><td>00:00:08</td><td>XEROX CORPORATION</td></tr> <tr><td>00:00:09</td><td>XEROX CORPORATION</td></tr> <tr><td>00:00:0A</td><td>OMRON TATEISI ELECTRONICS CO.</td></tr> <tr><td>00:00:0B</td><td>MATRIX CORPORATION</td></tr> <tr><td>00:00:0C</td><td>CISCO SYSTEMS, INC.</td></tr> <tr><td>00:00:0D</td><td>FIBRONICS LTD.</td></tr> <tr><td>00:00:0E</td><td>FUJITSU LIMITED</td></tr> <tr><td>00:00:0F</td><td>NEXT, INC.</td></tr> <tr><td>00:00:10</td><td>HIKES</td></tr> </tbody> </table>		MAC	Fabricante	00:00:00	XEROX CORPORATION	00:00:01	XEROX CORPORATION	00:00:02	XEROX CORPORATION	00:00:03	XEROX CORPORATION	00:00:04	XEROX CORPORATION	00:00:05	XEROX CORPORATION	00:00:06	XEROX CORPORATION	00:00:07	XEROX CORPORATION	00:00:08	XEROX CORPORATION	00:00:09	XEROX CORPORATION	00:00:0A	OMRON TATEISI ELECTRONICS CO.	00:00:0B	MATRIX CORPORATION	00:00:0C	CISCO SYSTEMS, INC.	00:00:0D	FIBRONICS LTD.	00:00:0E	FUJITSU LIMITED	00:00:0F	NEXT, INC.	00:00:10	HIKES
MAC	Fabricante																																				
00:00:00	XEROX CORPORATION																																				
00:00:01	XEROX CORPORATION																																				
00:00:02	XEROX CORPORATION																																				
00:00:03	XEROX CORPORATION																																				
00:00:04	XEROX CORPORATION																																				
00:00:05	XEROX CORPORATION																																				
00:00:06	XEROX CORPORATION																																				
00:00:07	XEROX CORPORATION																																				
00:00:08	XEROX CORPORATION																																				
00:00:09	XEROX CORPORATION																																				
00:00:0A	OMRON TATEISI ELECTRONICS CO.																																				
00:00:0B	MATRIX CORPORATION																																				
00:00:0C	CISCO SYSTEMS, INC.																																				
00:00:0D	FIBRONICS LTD.																																				
00:00:0E	FUJITSU LIMITED																																				
00:00:0F	NEXT, INC.																																				
00:00:10	HIKES																																				

Tabla 5: Historia de Usuario - Gestionar fabricantes de tarjetas de red y sus MACs

Historia de Usuario	
Número: 6	Nombre: Gestionar marcas y modelos de los dispositivos permitidos
Prioridad: Bajo	Riesgo en desarrollo: Medio
Iteración asignada: 3	Puntos estimados: 0.8
Descripción: El sistema debe permitirle al usuario que tenga permiso poder listar, insertar, modificar y eliminar marcas y modelos de los dispositivos permitidos.	
Observaciones: Un modelo solo puede estar asociado a una marca y una marca solo puede estar asociado a un tipo de dispositivo. El usuario debe estar previamente autenticado en el sistema.	

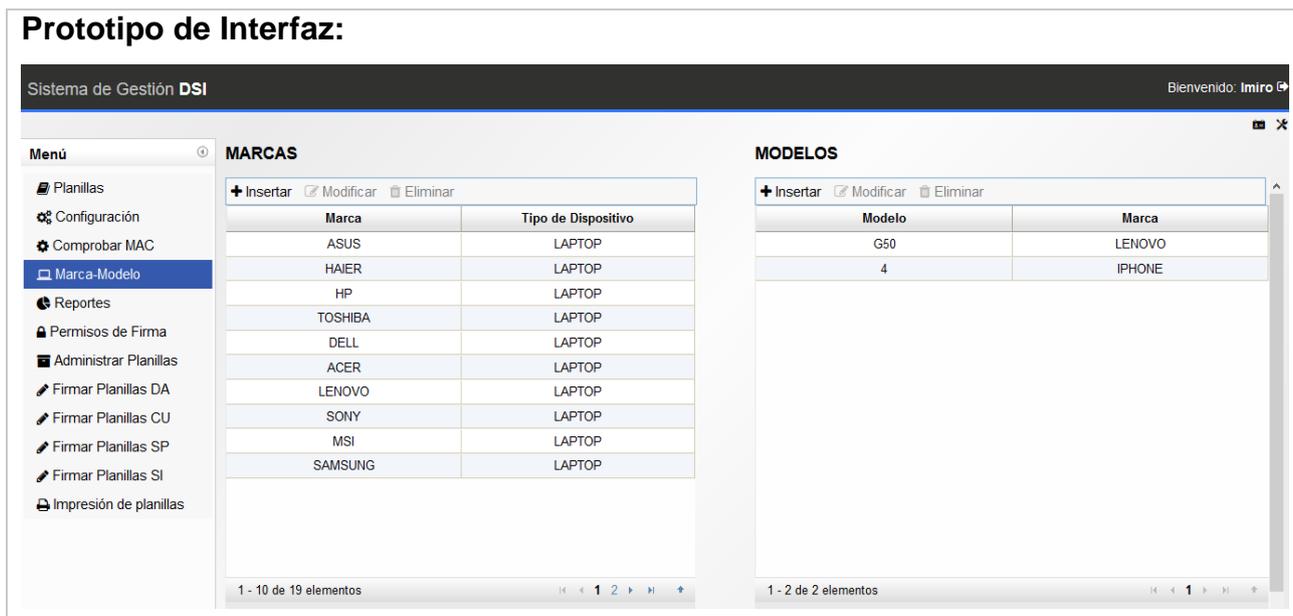


Tabla 6: Historia de Usuario - Gestionar marcas y modelos de los dispositivos permitidos

Historia de Usuario

Número: 7 **Nombre: Generar Reportes**

Prioridad: Baja **Riesgo en desarrollo: Alto**

Iteración asignada: 3 **Puntos estimados: 1**

Descripción: El sistema debe permitirle al usuario que tenga permiso poder ver y exportar la información de los reportes definidos.

Observaciones: El usuario deberá estar previamente autenticado en el sistema.

Prototipo de Interfaz:

The screenshot shows the 'Sistema de Gestión DSI' interface with the 'Reportes' menu item selected. It features four data tables:

- Cantidad de MAC por fabricantes (BD):** A table with columns 'Fabricantes' and 'Cantidad', listing CISCO SYSTEMS, INC. (519), APPLE (340), SAMSUNG ELECTRONICS CO.,LTD (205), ARRIS GROUP, INC. (174), and INTEL CORPORATE (140).
- Cantidad de MAC por fabricantes (UCI):** A table with columns 'Fabricantes' and 'Cantidad', listing XEROX CORPORATION (1), SIMTEL S.R.L. (1), and INES TEST AND MEASUREMENT GMBH & CO KG (1).
- Solicitudes de Planillas:** A table with columns 'Tipo', 'Cantidad Histórica', and 'Cantidad en 2016', showing 'Aprobadas' (3) and 'Cantidad de personas' (3).
- Solicitudes aprobadas por área:** A table with columns 'Área', 'Cantidad Histórica', and 'Cantidad en 2016', showing 'Centro de Informática Industrial' (2) and 'Facultad 2' (1).

Tabla 7: Historia de Usuario - Generar reportes

3.3 Planificación

En esta fase el cliente establece la prioridad de cada historia de usuario, y correspondientemente, los programadores realizan una estimación del esfuerzo necesario de cada una de ellas. Se toman acuerdos sobre el contenido de la primera entrega y se determina un cronograma en conjunto con el cliente. Esta fase dura unos pocos días. Las estimaciones de esfuerzo asociado a la implementación de las historias la establecen los programadores utilizando como medida el punto. Un punto, equivale a una semana ideal de programación. Las historias generalmente valen de 1 a 3 puntos (18).

3.3.1 Estimación de esfuerzo por Historias de Usuario

Para el desarrollo satisfactorio de la solución propuesta, se realizó una estimación de esfuerzo para cada una de las historias de usuario, arrojando los siguientes resultados:

Historia de Usuario	Puntos estimados
Procesar planillas de solicitud	3
Gestionar permisos de firmas	2
Gestionar configuraciones	0.2
Gestionar los tipos de dispositivos permitidos	0.4
Gestionar fabricantes de tarjetas de red y sus MACs	0.6
Gestionar marcas y modelos de los dispositivos permitidos	0.8
Generar Reportes	1

Tabla 8: Estimación de esfuerzo por Historias de Usuario

3.3.2 Plan de Iteraciones

En el plan de iteraciones se establece cuántas iteraciones serán necesarias realizar sobre el sistema para su consecución. Sin embargo, se precisa establecer el contenido de trabajo para todas y cada una de ellas y es aquí donde se establece el plan de iteraciones, regulando la cantidad de historias de usuario a implementar dentro del rango establecido por la estimación efectuada. Tomando como referencia los aspectos antes tratados la aplicación que se pretende construir se desarrollará en 3 iteraciones, explicada más detalladamente a continuación:

Iteración 1

La primera iteración del desarrollo del sistema, tendrá como objetivo la implementación de las funcionalidades básicas para la puesta en marcha del mismo. Se tendrán en cuenta la historia de usuario con prioridad de negocio alta. De manera general al finalizar esta iteración se habrá podido cumplir con las funcionalidades de la gestión de las planillas de solicitud, obteniéndose la primera versión del software que se le entregará al cliente.

Iteración 2

Durante la segunda iteración se seguirán implementando historias de usuario de prioridad media. Al finalizar esta iteración se habrá podido cumplir con la gestión de los permisos de firma. La versión de prueba referente a esta iteración, junto a las implementaciones anteriores, serán mostradas al cliente con el objetivo de realizar cambios en base a la opinión del mismo.

Iteración 3

Durante la tercera iteración se desarrollarán las historias de usuario de prioridad baja con las cuales se completarán todas las funcionalidades para las que está diseñado el sistema. Se podrá ver y exportar reportes de estadísticas, realizar la gestión de configuración, la gestión de los tipos de dispositivos permitidos, la gestión de fabricantes de tarjetas de red y la gestión de marcas y modelos. Finalizando esta iteración el sistema estará listo para entregarse al cliente completamente.

3.3.3 Plan de duración de las Iteraciones

Para conocer el tiempo real de la duración de las iteraciones del proyecto, así como las historias de usuario que serán implementadas en cada una de las mismas, la metodología XP propone la creación del Plan de Duración de las Iteraciones. Su propósito fundamental es conocer el tiempo que abarcará cada iteración y el orden en que serán implementadas las historias de usuario dentro de cada período.

Iteraciones	Historias de Usuario que se implementan	Duración
Iteración 1	Procesar Planillas de Solicitud.	3 semanas
Iteración 2	Gestionar permisos de firma.	2 semanas
Iteración 3	Gestionar Configuraciones.	3 semanas
	Gestionar Tipos de dispositivos permitidos.	
	Gestionar fabricantes de tarjetas de red y sus MACs.	
	Gestionar marcas y modelos de los tipos de dispositivos permitidos.	
	Generar Reportes.	

Tabla 9: Plan de duración de las iteraciones

3.3.4 Plan de entregas

El Plan de entrega no es más que el cronograma de las entregas de partes funcionales del software que serán hechas al cliente. A continuación se presenta el plan que comienza el lunes 14 de marzo de 2016:

Iteración	Fecha de entrega
1	1/04/2016
2	15/04/2016
3	6/05/2016

Tabla 10: Plan de entregas

3.4 Conclusiones del capítulo

En este capítulo se ha hecho referencia a las fases de Exploración y Planificación del sistema que fundamenta la presente investigación. Se han descrito los artefactos más importantes que la metodología de desarrollo propone para esta etapa y que sirven de base para las próximas etapas de desarrollo. Las fases que se detallaron en este capítulo son de gran importancia, pues marcan las pautas de la construcción del software, lográndose estimar el tiempo que tomará implementarlo, así como la prioridad de las versiones del sistema que serán entregadas al cliente, organizando de forma general el trabajo del equipo de desarrollo.

CAPÍTULO 4: DISEÑO E IMPLEMENTACIÓN

4.1 Introducción

En el presente capítulo se hace referencia al diseño de la aplicación y de la base de datos como punto de partida para la implementación del sistema. Se describen las tareas realizadas durante las tres iteraciones del desarrollo del software que se definieron anteriormente, de forma tal, que al finalizar cada una de ellas se entregará una parte funcional del software al cliente y este realizará las pruebas pertinentes para su aceptación final.

4.2 Diseño

XP establece prácticas especializadas que inciden directamente en la realización del diseño para lograr un sistema robusto y reutilizable tratando de mantener su simplicidad, es decir, crear un diseño evolutivo que se va mejorando incrementalmente y que permite hacer entregas pequeñas y frecuentes de valor para el cliente. A la hora de darle cumplimiento a la actividad de diseñar, XP no especifica ninguna técnica de modelado. Pueden utilizarse indistintamente sencillos esquemas en una pizarra, diagramas de clases utilizando UML o tarjetas CRC (Clase, Responsabilidad y Colaboración) siempre que sean útiles, tributen a la comprensión y no requieran mucho tiempo en su creación.

Como base para el desarrollo de la aplicación propuesta se utilizó el marco de trabajo Symfony 2 que implementa, como lo hacen muchos otros, el patrón arquitectónico MVC (Modelo Vista Controlador) que obliga a organizar el código de acuerdo a sus convenciones. Symfony 2 proporciona una estructura en forma de árbol de archivos para organizar de forma lógica todos esos contenidos, además de ser consistente con la arquitectura MVC utilizada y con la agrupación de los directorios de la forma proyecto / src / bundle. Cada vez que se crea un nuevo proyecto, aplicación o módulo, se genera de forma automática la parte correspondiente de esa estructura. Además, la estructura se puede personalizar completamente, para reorganizar los archivos y directorios o para cumplir con las exigencias de organización de un cliente.

4.2.1 Patrón Arquitectónico

Un patrón arquitectónico describe una categoría del sistema que contiene: un conjunto de componentes (por ejemplo, una base de datos, módulos computacionales) que realizan una función requerida por el sistema; un conjunto de conectores que posibilitan la comunicación, la coordinación y la cooperación entre los componentes; restricciones que definen cómo se pueden integrar los componentes que forman el sistema; y modelos semánticos que permiten al diseñador entender las propiedades globales de un sistema para analizar las propiedades conocidas de sus partes constituyentes. (20)

4.2.1.1 Modelo Vista Controlador (MVC)

Symfony2, framework de desarrollo seleccionado, basa su funcionamiento interno en la famosa arquitectura Modelo-Vista-Controlador, utilizada por la mayoría de los frameworks web. El patrón de arquitectura de software MVC separa los datos y la lógica de negocio de una aplicación de la interfaz de usuario y el módulo encargado de gestionar los eventos y las comunicaciones. Este patrón de arquitectura de software se basa en las ideas de reutilización de código y la separación de conceptos, características que buscan facilitar la tarea de desarrollo de aplicaciones y su posterior mantenimiento.

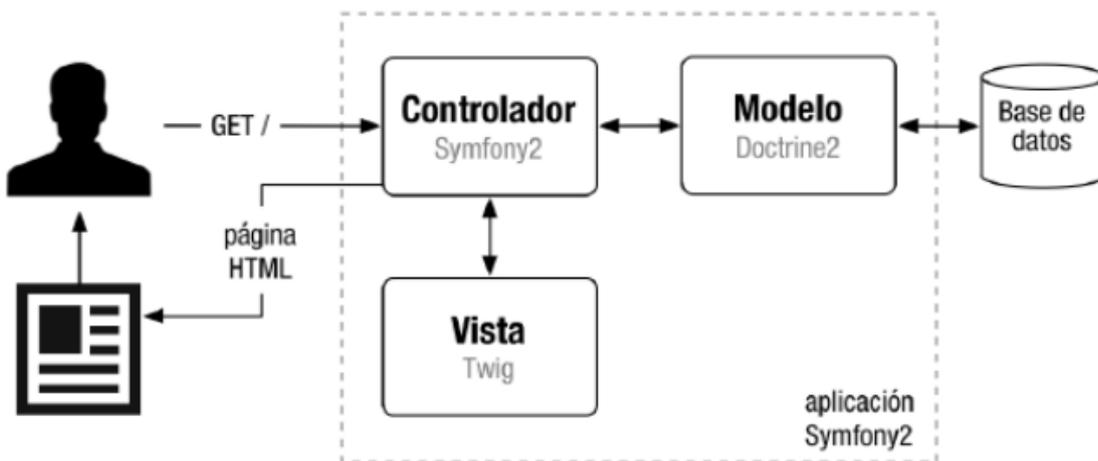


Figura 2: Modelo-Vista-Controlador (tomado del libro Desarrollo web ágil con Symfony2)

4.2.2 Patrones de diseño

Un patrón de diseño provee un esquema para refinar los subsistemas o componentes de un sistema de software.

Los patrones de diseño pretenden proporcionar catálogos de elementos reusables en el diseño de sistemas software, evitar la reiteración en la búsqueda de soluciones a problemas ya conocidos y solucionados anteriormente, formalizar un vocabulario común entre diseñadores, estandarizar el modo en que se realiza el diseño y facilitar el aprendizaje de las nuevas generaciones de diseñadores condensando conocimiento ya existente. (21)

Patrones GRASP

General Responsibility Assignment Software Patterns (GRASP) nos da unos principios generales para asignar responsabilidades y se utiliza sobre todo en la realización de diagramas de interacción. Una vez que tenemos el Modelo de dominio hay que decidir qué métodos añadir y dónde (parte esencial del desarrollo Orientado a Objeto). Básicamente las responsabilidades de un objeto son conocer y hacer. Dichas responsabilidades implicarán más o menos métodos y clases.

Experto:

Su objetivo es asignar responsabilidades al experto de la información, es decir, a la clase que tiene la información necesaria para llevar la tarea a cabo. El uso de este patrón se pone en práctica en las clases controladoras ya que solo ellas cuentan con la información necesaria para cumplir con la responsabilidad sobre los elementos del negocio.

Bajo Acoplamiento:

Acoplamiento indica que tan fuertemente está conectada una clase con otra, tiene conocimiento de, o influye sobre otra clase, una clase con bajo acoplamiento no depende de otras clases. Su objetivo es asignar responsabilidades de tal manera que el acoplamiento sea el menor posible. En la solución este patrón se pone en práctica debido a que cada clase tiene relación con un número relativamente pequeño de clases y además fue un factor fundamental dentro del diseño de la solución.

Alta Cohesión:

Alta cohesión implica lo relacionadas que están las responsabilidades de una clase, o una clase con responsabilidades altamente relacionadas y que no lleva a cabo gran cantidad de trabajo. Su objetivo es poder asignar responsabilidades procurando que la cohesión sea lo más alta posible. Se hizo uso de este patrón en la solución en las clases controladoras ya que se le asignan a cada una las funcionalidades que solo ellas pueden realizar.

Creador:

El patrón creador ayuda a identificar quién debe ser el responsable de la creación o instanciación de nuevos objetos o clases. Éste patrón nos dice que la nueva instancia podrá ser creada por una clase si:

- ✓ Contiene o agrega la clase.
- ✓ Almacena la instancia en algún sitio (por ejemplo una base de datos).
- ✓ Tiene la información necesaria para realizar la creación del objeto (es 'Experta').
- ✓ Usa directamente las instancias creadas del objeto.

En la solución se usó este patrón en las clases controladoras ya que solo ellas tienen la responsabilidad de crear o instanciar un objeto.

Controlador:

Un controlador es un objeto responsable del manejo de los eventos del sistema, que no pertenece a la interfaz del usuario, el controlador recibe la solicitud del y coordina su realización delegando a otros objetos. Se hizo uso de este patrón ya que la propia arquitectura definida por Symfony2

(Modelo-Vista-Controlador) provee a los usuarios de crear clases controladoras que tienen como objetivo controlar las acciones que realiza el usuario con las interfaces de la aplicación y dar respuesta a las peticiones realizadas.

4.2.3 Tarjetas CRC

La metodología XP propone representar las clases mediante tarjetas CRC (Class-Responsibility-Collaboration). El objetivo de las tarjetas CRC es hacer, mediante tarjetas, un inventario de las clases que se va a necesitar para implementar el sistema y la forma en que van a interactuar, así se pretende facilitar el análisis y discusión de las mismas por parte de varios actores del equipo de proyecto con el objetivo de que el diseño sea lo más simple posible verificando las especificaciones del sistema. Cada tarjeta representa una clase con su nombre en la parte superior, en la sección inferior izquierda están descritas las responsabilidades y a la derecha las clases que le sirven de soporte.

Clase: AreaController	
Responsabilidades:	Colaboradores:
<ul style="list-style-type: none"> ✓ Devolver las áreas registradas en el sistema. 	MTArea

Tabla 11: Tarjeta CRC para la clase AreaController

Clase: ConfiguracionController	
Responsabilidades:	Colaboradores:
<ul style="list-style-type: none"> ✓ Listar los valores de configuración. ✓ Modificar los valores de configuración. 	MTConfiguracion. ConfiguracionRepository.

Tabla 12: Tarjeta CRC para la clase ConfiguracionController

Clase: EstadisticasController	
Responsabilidades:	Colaboradores:
<ul style="list-style-type: none"> ✓ Listar la cantidad de MAC que existen por cada fabricante. ✓ Listar la cantidad de MAC que existen por cada fabricante dentro de la universidad. ✓ Listar la cantidad histórica y la cantidad del año en curso de solicitudes aprobadas. ✓ Listar la cantidad y la cantidad del año en curso de personas que tienen al menos una solicitud de planilla aprobada. 	MTMacVendors MTPlanilla

Tabla 13: Tarjeta CRC para la clase EstadisticasController

Clase: MacvendorsController	
Responsabilidades: <ul style="list-style-type: none"> ✓ Listar los fabricantes y sus MAC asociadas. ✓ Listar las MAC que no han sido comprobadas. ✓ Comprobar MAC con la API. 	Colaboradores: <ul style="list-style-type: none"> MTMacVendors. MacvendorsRepository. MTPlanilla.

Tabla 14: Tarjeta CRC para la clase MacvendorsController

Clase: MarcaController	
Responsabilidades: <ul style="list-style-type: none"> ✓ Listar las Marcas. ✓ Crear las Marcas. ✓ Modificar las Marcas. ✓ Eliminar las Marcas. ✓ Devolver las marcas asociadas a un tipo de dispositivo. 	Colaboradores: <ul style="list-style-type: none"> MTMarca. MarcaRepository.

Tabla 15: Tarjeta CRC para la clase MarcaController

Clase: ModeloController	
Responsabilidades: <ul style="list-style-type: none"> ✓ Listar los Modelos. ✓ Crear los Modelos. ✓ Modificar los Modelos. ✓ Eliminar los Modelos. ✓ Devolver los modelos asociados a un tipo de marca. 	Colaboradores: <ul style="list-style-type: none"> MTModelo. ModeloRepository.

Tabla 16: Tarjeta CRC para la clase ModeloController

Clase: PDFController	
Responsabilidades: <ul style="list-style-type: none"> ✓ Descargar la planilla en formato pdf para su posterior impresión. 	Colaboradores: <ul style="list-style-type: none"> MTPlanilla. MTMarca. MTTipoDispositivosPermitidos.

Tabla 17: Tarjeta CRC para la clase PDFController

Clase: PermisoController	
Responsabilidades:	Colaboradores:

<ul style="list-style-type: none"> ✓ Listar las relaciones entre los usuarios y las áreas a las cuales tienen permiso de firma. ✓ Crear una relación entre un usuario y un área. ✓ Eliminar la relación entre un usuario y un área. 	<p>MTUsuario_Area. MTUsuario. MTArea.</p>
--	---

Tabla 18: Tarjeta CRC para la clase PermisoController

Clase: PlanillaController	
Responsabilidades: <ul style="list-style-type: none"> ✓ Listar las Planillas. ✓ Crear planillas. ✓ Aceptar planillas. ✓ Denegar planillas. ✓ Cancelar planillas. ✓ Determinar si una MAC es válida. 	Colaboradores: <p>MTPlanilla. PlanillaRepository. MTUsuario. MTMarca. MTUsuario. MTArea. MTModelo. MTMacVendors. MTUsuario_Area.</p>

Tabla 19: Tarjeta CRC para la clase PlanillaController

Clase: TipoDispositivosController	
Responsabilidades: <p>Listar los Tipos de dispositivos permitidos. Crear los Tipos de dispositivos permitidos. Modificar los Tipos de dispositivos permitidos. Eliminar los Tipos de dispositivos permitidos.</p>	Colaboradores: <p>MTTipoDispositivosPermitidos. TiposDispositivosRepository.</p>

Tabla 20: Tarjeta CRC para la clase TipoDispositivosController

Clase: UsuarioController	
Responsabilidades: <p>Devolver los Usuarios.</p>	Colaboradores: <p>MTUsuario.</p>

Tabla 21: Tarjeta CRC para la clase UsuarioController

Clase: MTArea	
Responsabilidades:	Colaboradores:

<ul style="list-style-type: none"> ✓ Obtener el nombre del área. ✓ Modificar el nombre del área. 	
--	--

Tabla 22: Tarjeta CRC para la clase MTArea

Clase: MTConfiguracion	
Responsabilidades: <ul style="list-style-type: none"> ✓ Obtener la cantidad de dispositivos permitidos por persona. ✓ Modificar la cantidad de dispositivos permitidos por persona. ✓ Obtener la duración de una solicitud. ✓ Modificar la duración de una solicitud. 	Colaboradores:

Tabla 23: Tarjeta CRC para la clase MTConfiguracion

Clase: MTMacVendors	
Responsabilidades: <ul style="list-style-type: none"> ✓ Obtener la mac de los Macvendors. ✓ Modificar la mac de los Macvendors. ✓ Obtener el fabricante de los Macvendors. ✓ Modificar el fabricante de los Macvendors. 	Colaboradores:

Tabla 24: Tarjeta CRC para la clase MTMacVendors

Clase: MTMarca	
Responsabilidades: <ul style="list-style-type: none"> ✓ Obtener el nombre de la marca. ✓ Modificar el nombre de la marca. ✓ Obtener el tipo de dispositivo al que pertenece la marca ✓ Modificar el tipo de dispositivo al que pertenece la marca. 	Colaboradores: MTTipoDispositivosPermitidos

Tabla 25: Tarjeta CRC para la clase MTMarca

Clase: MTModelo	
Responsabilidades: <ul style="list-style-type: none"> ✓ Obtener el nombre del modelo. ✓ Modificar el nombre del modelo. 	Colaboradores: MTMarca

<ul style="list-style-type: none"> ✓ Obtener la marca al que pertenece el modelo. ✓ Modificar la marca al que pertenece el modelo. 	
--	--

Tabla 26: Tarjeta CRC para la clase MTModelo

Clase: MTPlanilla	
Responsabilidades: <ul style="list-style-type: none"> ✓ Obtener y modificar la MAC del dispositivo asociado a la planilla. ✓ Obtener y modificar el número de serie del dispositivo asociado a la planilla. ✓ Obtener y modificar la fecha de solicitud de la planilla. ✓ Obtener y modificar el estado de las aprobaciones de las planillas. ✓ Obtener y modificar el usuario que solicita la planilla. ✓ Obtener y modificar el modelo del dispositivo asociado a la planilla. ✓ Obtener y modificar el estado de aprobación en que se encuentra la MAC. ✓ Obtener y modificar el estado de impresión de la planilla. 	Colaboradores: <p>MTUsuario MTModelo</p>

Tabla 27: Tarjeta CRC para la clase MTPlanilla

Clase: MTTipoDispositivosPermitidos	
Responsabilidades: <p>Obtener el nombre del tipo de dispositivo permitido.</p> <p>Modificar el nombre del tipo de dispositivo permitido.</p>	Colaboradores:

Tabla 28: Tarjeta CRC para la clase MTTipoDispositivosPermitidos

Clase: MTUsuario	
Responsabilidades:	Colaboradores:

<ul style="list-style-type: none"> ✓ Obtener y modificar el nombre del usuario. ✓ Obtener y modificar los apellidos del usuario. ✓ Obtener y modificar el carnet de identidad del usuario. ✓ Obtener y modificar el solapín del usuario. ✓ Obtener y modificar el área del usuario. ✓ Obtener y modificar la dirección del usuario. ✓ Obtener y modificar el municipio del usuario. ✓ Obtener y modificar la provincia del usuario. ✓ Obtener y modificar el teléfono del usuario. ✓ Obtener y modificar el tipo de personal del usuario. 	
---	--

Tabla 29: Tarjeta CRC para la clase MTUsuario

Clase: MTUsuario_Area	
Responsabilidades: <ul style="list-style-type: none"> ✓ Obtener y modificar el usuario relacionado con el área. ✓ Obtener y modificar el área relacionada con el usuario. 	Colaboradores: MTUsuario. MTArea.

Tabla 30: Tarjeta CRC para la clase MTUsuario_Area

Clase: ConfiguracionRepository	
Responsabilidades: <ul style="list-style-type: none"> ✓ Listar los valores de la configuración. 	Colaboradores: MTConfiguracion

Tabla 31: Tarjeta CRC para la clase ConfiguracionRepository

Clase: MacvendorsRepository	
Responsabilidades: <ul style="list-style-type: none"> ✓ Listar los MacVendors dado un orden. 	Colaboradores: MTMacVendors

<ul style="list-style-type: none"> ✓ Obtener la cantidad de fabricantes de MAC que existen en la base de datos. 	
--	--

Tabla 32: Tarjeta CRC para la clase MacvendorsRepository

Clase: MarcaRepository	
Responsabilidades: <ul style="list-style-type: none"> ✓ Listar las Marcas dado un orden. ✓ Obtener la cantidad de marcas que existen en la base de datos. 	Colaboradores: MTMarca

Tabla 33: Tarjeta CRC para la clase MarcaRepository

Clase: ModeloRepository	
Responsabilidades: <ul style="list-style-type: none"> ✓ Listar los Modelos dado un orden. ✓ Obtener la cantidad de modelos que existen en la base de datos. 	Colaboradores: MTModelo

Tabla 34: Tarjeta CRC para la clase ModeloRepository

Clase: PermisoRepository	
Responsabilidades: <ul style="list-style-type: none"> ✓ Listar las relaciones entre los usuarios y las áreas dado un orden. ✓ Obtener la cantidad de relaciones entre los usuarios y las áreas que existen en la base de datos. 	Colaboradores: MTUsuario_Area.

Tabla 35: Tarjeta CRC para la clase PermisoRepository

Clase: PlanillaRepository	
Responsabilidades: <ul style="list-style-type: none"> ✓ Listar todas las planillas dado un orden. ✓ Listar todas las planillas impresas. ✓ Listar todas las planillas de un usuario. ✓ Listar todas las planillas que no se hayan aprobado de una determinada área. 	Colaboradores: MTPlanilla

Tabla 36: Tarjeta CRC para la clase PlanillaRepository

Clase: TiposDispositivosRepository	
Responsabilidades:	Colaboradores:

- | | |
|---|------------------------------|
| ✓ Listar los tipos de dispositivos permitidos dados un orden. | MTTipoDispositivosPermitidos |
|---|------------------------------|

Tabla 37: Tarjeta CRC para la clase TiposDispositivosRepository

4.2.4 Modelo de Datos

Un modelo de datos es una colección de herramientas conceptuales para describir los datos, las relaciones, la semántica y las restricciones de consistencia. (22)

El modelo de datos correspondiente al sistema consta de un total de 9 tablas. A continuación se muestra en la figura 3 el modelo de dato que se obtuvo a partir de las clases generadas en las tarjetas CRC:

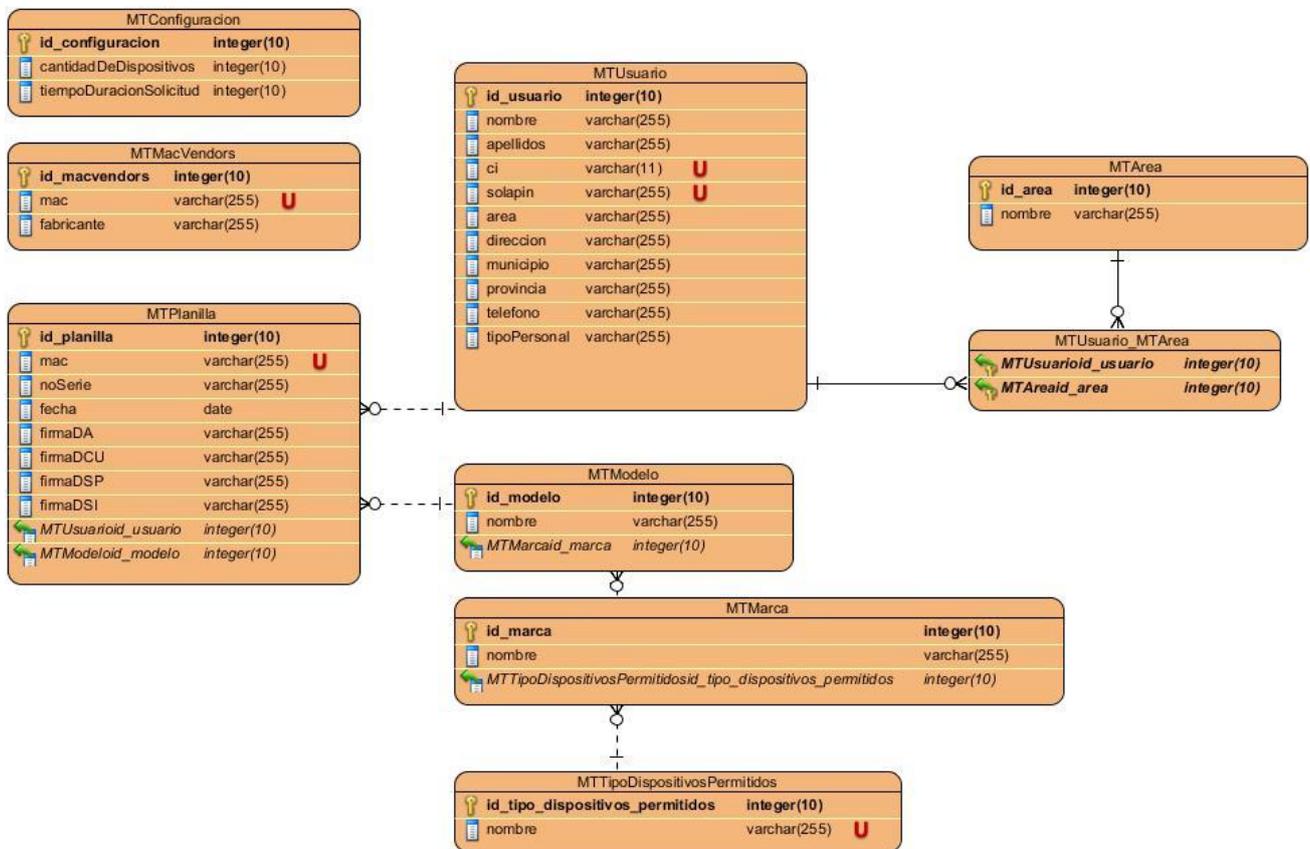


Figura 3: Modelo de datos

El modelo de datos mostrado anteriormente refleja los conceptos, las relaciones y las reglas del dominio estudiado, con el objetivo de darle respuesta al problema afrontado por el equipo.

4.3 Implementación

Como se ha detallado anteriormente un proyecto desarrollado en XP se divide en iteraciones para realizar la codificación, de manera que se puede entregar una versión funcional del software al

cliente, que aunque no esté completo en su totalidad, irá creciendo ciclo a ciclo. En cada iteración, se implementarán las historias de usuario definidas previamente en el Plan de Iteraciones. Se define además un conjunto de tareas, que deberán realizar los programadores para llevar a cabo la construcción del sistema.

Implementación de la 1ra Iteración.

Durante la primera iteración de la construcción del software se implementaron las historias de usuario que son de prioridad alta para poner en marcha el sistema, donde se obtuvo la primera versión del mismo, que posteriormente fue aprobada por el cliente. A continuación se presenta en la Tabla 38 la tarea de ingeniería “Solicitar planilla”. El resto de las tareas de ingeniería correspondientes a la primera iteración se pueden encontrar detalladas en el Anexo 1.

Tarea de ingeniería	
Nombre: Solicitar planilla	
HU: Procesar planillas de solicitud	Puntos estimados: 0.4
Fecha de inicio: 16/03/2016	Fecha de fin: 17/03/2016
Descripción: Un usuario puede solicitar una planilla llenando un formulario que se le muestra. Debe proporcionarle al sistema el tipo de dispositivo que desea registrar, la marca, el modelo, la MAC y el número de serie. Para completar los demás campos de la planilla que son datos del usuario (nombres, apellidos, usuario, área a la que pertenece, carnet de identidad, solapín, municipio, provincia, teléfono, tipo de personal) se deberá consumir estos de un servicio web. Una vez que se envíe la información se debe comprobar que todos los campos han sido completados con datos válidos. Si todos los campos fueron válidos se debe insertar en la base de datos esta planilla. Si no son válidos se debe mostrar un señalamiento del error.	

Tabla 38: Tarea de Ingeniería Solicitar planilla

Implementación de la 2da Iteración.

Durante la implementación de la segunda iteración del software se perfeccionaron las funcionalidades de la primera entrega y se continuó con el desarrollo de las historias de usuario que tienen prioridad media. A continuación se presenta en la Tabla 39 la tarea de ingeniería “Insertar permisos de firma”. El resto de las tareas de ingeniería correspondientes a la segunda iteración se pueden encontrar detalladas en el Anexo 2.

Tarea de ingeniería	
Nombre: Insertar permisos de firma	
HU: Gestionar permisos de firmas	Puntos estimados: 1
Fecha de inicio: 4/04/2016	Fecha de fin: 8/04/2016
Descripción: Un usuario que tenga autorización puede insertar permisos de firma. Esto se realizará mediante un formulario que dará a escoger un usuario y las áreas a las cuales se le quieren dar permiso de firma. Una vez seleccionados el usuario y las áreas deben insertarse en la base de datos estas relaciones.	

Tabla 39: Tarea de Ingeniería Insertar permisos de firma

Implementación de la 3ra Iteración.

Una vez concluida la implementación de las historias de usuario de la tercera iteración de la construcción del software, se obtuvo la versión completa del producto para ser entregado al cliente y listo para usarse en condiciones reales. A continuación se presenta en la Tabla 40 un ejemplo de la tarea de ingeniería “Mostrar configuración” realizada en la tercera iteración. Las demás tareas de ingeniería que se realizaron para el logro de este objetivo se pueden observar en el Anexo 3.

Tarea de ingeniería	
Nombre: Mostrar configuración	
HU: Gestionar configuraciones	Puntos estimados: 0.1
Fecha de inicio: 18/04/2016	Fecha de fin: 18/04/2016
Descripción: Un usuario que tenga autorización puede ver mediante una tabla la cantidad de dispositivos permitidos por persona y el tiempo de validez de una planilla de solicitud. Los valores por defecto que debe cargar el sistema cuando se despliegue serán de 1 dispositivo permitido por persona y 1 año de validez para una planilla.	

Tabla 40: Tarea de Ingeniería Mostrar configuración

4.4 Conclusiones del capítulo

En este capítulo se definió el diseño del sistema que será implementado y se construyó el modelo de datos que se utilizará, con el objetivo de lograr un mayor entendimiento. Se describieron los elementos esenciales de la arquitectura de la solución propuesta definiéndose como patrón arquitectónico Modelo-Vista-Controlador para garantizar una mejor organización en el sistema. Las

tareas de ingeniería y las tarjetas CRC definidas posibilitaron implementar la aplicación de una forma más organizada. Al concluir esta etapa se obtuvo la versión completa del sistema con lo que se da por terminado el desarrollo de la solución propuesta.

CAPÍTULO 5: VALIDACIÓN DE PROPUESTA

5.1 Introducción

La metodología XP enfatiza mucho los aspectos relacionados con las pruebas, clasificándolas en diferentes tipos y funcionalidades específicas, indicando quién, cuándo y cómo deben ser implementadas y ejecutadas. Según XP se debe ser muy estricto con las pruebas. Sólo se deberá liberar una nueva versión si esta ha pasado con el cien por ciento de la totalidad de las pruebas. En caso contrario se empleará el resultado de estas para identificar el error y solucionarlo con mecanismos ya definidos (23). En el presente capítulo se exponen las pruebas unitarias y de aceptación que se le realizaron al sistema.

5.1.1 Pruebas unitarias

Las pruebas unitarias aseguran que un único componente de la aplicación produce una salida correcta para una determinada entrada. Este tipo de pruebas validan la forma en la que las funciones y métodos trabajan en cada caso particular. Las pruebas unitarias se encargan de un único caso cada vez, lo que significa que un único método puede necesitar varias pruebas unitarias si su funcionamiento varía en función del contexto (24).

Para validar el cumplimiento de las funcionalidades del sistema construido, se realizó una prueba unitaria por cada una de estas. Se utilizó la librería PHPUnit que permite realizar este tipo de pruebas de forma automática.

En la primera iteración se realizaron un conjunto de 23 pruebas unitarias. A continuación se muestran los resultados obtenidos después de haberlas realizado.

```
C:\xampp\htdocs\Tesis_MT>phpunit -c app
PHPUnit 4.0.0 by Sebastian Bergmann.

Configuration read from C:\xampp\htdocs\Tesis_MT\app\phpunit.xml.dist

The Xdebug extension is not loaded. No code coverage will be generated.

.....

Time: 331 ms, Memory: 5.50MB
OK (23 tests, 23 assertions)
```

Figura 4: Resultados obtenidos de las pruebas unitarias en 1era iteración

En la segunda iteración se realizaron un total de 17 pruebas unitarias. A continuación se muestran los resultados obtenidos después de haberlas realizado.

```
C:\xampp\htdocs\Tesis_MT>phpunit -c app
PHPUnit 4.0.0 by Sebastian Bergmann.

Configuration read from C:\xampp\htdocs\Tesis_MT\app\phpunit.xml.dist

The Xdebug extension is not loaded. No code coverage will be generated.

.....

Time: 249 ms, Memory: 5.50MB

OK (17 tests, 17 assertions)
```

Figura 5: Resultados obtenidos de las pruebas unitarias en 2da iteración

En la tercera iteración se realizaron un total de 15 pruebas unitarias. A continuación se muestran los resultados obtenidos después de haberlas realizado.

```
C:\xampp\htdocs\Tesis_MT>phpunit -c app
PHPUnit 4.0.0 by Sebastian Bergmann.

Configuration read from C:\xampp\htdocs\Tesis_MT\app\phpunit.xml.dist

The Xdebug extension is not loaded. No code coverage will be generated.

.....

Time: 234 ms, Memory: 5.00MB

OK (15 tests, 15 assertions)
```

Figura 6: Resultados obtenidos de las pruebas unitarias en 3era iteración

Tras haber aplicado las pruebas unitarias a la aplicación en cada una de las iteraciones se obtuvo un resultado completamente satisfactorio, que permite verificar que el código de la aplicación produce una salida correcta para determinadas entradas.

A continuación se muestra un fragmento de código de las pruebas unitarias realizadas haciendo uso de la librería PHPUnit.

```

public function testValidarModelo()
{
    $modelo = new MTModelo();
    $modelo->setNombre(null);
    $modelo->setMarca(null);
    $listaErrores = $this->validator->validate($modelo);
    $this->assertEquals(1, $listaErrores->count(),
        'Ningún campo puede estar vacío'
    );
}

public function testValidarPlanilla()
{
    $planilla = new MTPlanilla();
    $planilla->setMac('XX:XX:XX:XX');
    $planilla->setModelo(null);
    $planilla->setNoSerie(null);
    $listaErrores = $this->validator->validate($planilla);
    $this->assertEquals(3, $listaErrores->count(),
        'Ningún campo puede estar vacío y la MAC debe tener 17 caracteres'
    );
}

public function testValidarTipoDispositivosPermitidos()
{
    $dispositivos = new MTTipoDispositivosPermitidos();
    $dispositivos->setNombre(null);
    $listaErrores = $this->validator->validate($dispositivos);
    $this->assertEquals(1, $listaErrores->count(),
        'Ningún campo puede estar vacío'
    );
}

```

Figura 7: Fragmento de código de pruebas unitarias

5.1.2 Pruebas de aceptación

Las pruebas de aceptación o funcionales validan partes de las aplicaciones. Estas pruebas simulan la navegación del usuario, realizan peticiones y comprueban los elementos de la respuesta, tal y como lo haría manualmente un usuario para validar que una determinada acción hace lo que se supone que tiene que hacer (25).

Son supervisadas por el cliente basándose en las funcionalidades tomadas de las historias de usuario. En todas las iteraciones, cada una de las historias de usuario seleccionadas por el cliente deberá tener una o más pruebas de aceptación, de las cuales deberán determinar los casos de prueba e identificar los errores que serán corregidos (23).

Pruebas de aceptación realizadas:

Para el desarrollo del presente módulo se realizaron un total de 25 pruebas de aceptación con el objetivo de garantizar que las funcionalidades y la satisfacción del cliente han sido cumplidas.

Prueba de aceptación	
Código: HU1_P1	HU: Procesar planillas de solicitud.
Nombre: Listar planillas.	
Descripción: Probar que el sistema muestre el tipo de dispositivo, la marca, el modelo, la MAC, el número de serie y el estado de una planilla.	
Condiciones de ejecución: El usuario debe estar previamente autenticado.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Planillas.	
Resultado esperado: El sistema debe mostrar el tipo de dispositivo, la marca, el modelo, la MAC, el número de serie y el estado de una planilla.	
Resultado obtenido: El sistema muestra el tipo de dispositivo, la marca, el modelo, la MAC, el número de serie y el estado de una planilla.	
Evaluación de la respuesta: El cliente informa de una no conformidad donde recomienda que se le muestre en la columna "Estado" el estado de aprobación de cada directivo.	

Tabla 41: Prueba de aceptación: Listar planillas

Prueba de aceptación	
Código: HU1_P2	HU: Procesar planillas de solicitud.
Nombre: Solicitar planilla	
Descripción: Probar que el sistema permita al usuario solicitar una planilla.	
Condiciones de ejecución: El usuario debe estar previamente autenticado.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Planillas. Oprimir el botón solicitar. Completar los campos. Oprimir el botón enviar.	
Resultado esperado: El sistema deberá insertar en la base de datos la solicitud realizada y mostrarle al usuario las planillas con la nueva inserción.	
Resultado obtenido: El sistema inserta en la base de datos la solicitud realizada y muestra al usuario las planillas con la nueva inserción.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 42: Prueba de aceptación: Solicitar planilla

Prueba de aceptación	
Código: HU1_P3	HU: Procesar planillas de solicitud.
Nombre: Cancelar planilla	
Descripción: Probar que el sistema permita al usuario cancelar una planilla.	
Condiciones de ejecución: El usuario debe estar previamente autenticado.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Planillas. Seleccionar la o las planillas a cancelar. Oprimir en el botón Cancelar.	
Resultado esperado: El sistema deberá eliminar en la base de datos la solicitud seleccionada y mostrarle al usuario las planillas con la nueva eliminación.	
Resultado obtenido: El sistema elimina en la base de datos la planilla seleccionada y muestra al usuario sus planillas teniendo en cuenta que no se muestra la planilla eliminada.	
Evaluación de la respuesta: El cliente informa de una no conformidad donde recomienda que se le muestre un mensaje de confirmación antes de cancelar la planilla.	

Tabla 43: Prueba de aceptación: Cancelar planilla

Prueba de aceptación	
Código: HU1_P4	HU: Procesar planillas de solicitud.
Nombre: Ver planilla en formato pdf	
Descripción: Probar que el sistema permita al usuario ver una planilla en formato pdf.	
Condiciones de ejecución: El usuario debe estar previamente autenticado.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Planillas. Seleccionar la planilla que desea ver en formato pdf. Oprimir en el botón Ver PDF.	
Resultado esperado: El sistema deberá mostrar en formato pdf la planilla seleccionada.	
Resultado obtenido: El sistema muestra en formato pdf la planilla seleccionada.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 44: Prueba de aceptación: Ver planilla en formato pdf

Prueba de aceptación	
Código: HU1_P5	HU: Procesar planillas de solicitud.
Nombre: Firmar como directivo	

Descripción: Probar que el sistema permita a los usuarios que tengan permiso de firma poder aprobar o rechazar una planilla.
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para firmar planillas.
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Firmar Planillas DA, Firmar Planillas CU, Firmar Planillas SP o Firmar Planillas SI, en dependencia del permiso que tenga. Seleccionar la planilla que desea aprobar o rechazar. Oprimir en el botón Aprobar o Rechazar.
Resultado esperado: El sistema deberá cambiar el estado de la planilla seleccionada a aprobada o rechazada, en dependencia del botón presionado.
Resultado obtenido: El sistema cambia el estado de la planilla seleccionada a aprobada o rechazada, en dependencia del botón presionado.
Evaluación de la respuesta: El cliente informa de una no conformidad donde recomienda que se le muestre en la columna "Usuario" la foto del usuario que realiza la solicitud.

Tabla 45: Prueba de aceptación: Firmar como directivo

Prueba de aceptación	
Código: HU2_P6	HU: Gestionar permisos de firma
Nombre: Mostrar permisos de firma.	
Descripción: Probar que el sistema muestre el usuario y el área sobre la cual tiene permiso de firma.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para ver permisos de firma.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Permisos de firma.	
Resultado esperado: El sistema deberá mostrar todos los permisos de firma que se han insertado. Debe mostrar el usuario y el área sobre la cual tiene permiso de firma.	
Resultado obtenido: El sistema muestra todos los permisos de firma que se han insertado. Muestra el usuario y el área sobre la cual tiene permiso de firma.	
Evaluación de la respuesta: El cliente informa de una no conformidad donde detecta que existen errores ortográficos.	

Tabla 46: Prueba de aceptación: Mostrar permisos de firma

Prueba de aceptación

Código: HU2_P7	HU: Gestionar permisos de firma
Nombre: Insertar permisos de firma.	
Descripción: Probar que el sistema permita a un usuario insertar relaciones de permisos de firma.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para otorgar permisos de firma.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Permisos de firma. Oprimir el botón Insertar. Seleccionar el usuario al cual desea otorgarle permisos de firma. Seleccionar las áreas sobre las cuales va a tener permisos de firma. Oprimir el botón enviar.	
Resultado esperado: El sistema deberá insertar las relaciones creadas.	
Resultado obtenido: El sistema inserta las relaciones creadas.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 47: Prueba de aceptación: Insertar permisos de firma

Prueba de aceptación	
Código: HU2_P8	HU: Gestionar permisos de firma
Nombre: Eliminar permisos de firma.	
Descripción: Probar que el sistema permita a un usuario eliminar relaciones de permisos de firma.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para eliminar permisos de firma.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Permisos de firma. Seleccionar las relaciones que desea eliminar. Oprimir el botón Eliminar.	
Resultado esperado: El sistema deberá eliminar todas las relaciones seleccionadas.	
Resultado obtenido: El sistema elimina todas las relaciones seleccionadas.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 48: Prueba de aceptación: Eliminar permisos de firma

Prueba de aceptación	
Código: HU3_P9	HU: Gestionar configuraciones

Nombre: Mostrar configuración
Descripción: Probar que el sistema permita a un usuario ver la configuración
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para ver la configuración.
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Configuración.
Resultado esperado: El sistema deberá mostrar la cantidad de dispositivos permitidos por persona y el tiempo de duración válido de una planilla.
Resultado obtenido: El sistema muestra la cantidad de dispositivos permitidos por persona y el tiempo de duración válido de una planilla.
Evaluación de la respuesta: Prueba Satisfactoria.

Tabla 49: Prueba de aceptación: Mostrar configuración

Prueba de aceptación	
Código: HU3_P10	HU: Gestionar configuraciones
Nombre: Modificar configuración	
Descripción: Probar que el sistema permita a un usuario modificar la configuración	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para modificar la configuración.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Configuración. Seleccionar la fila que tiene los valores. Oprimir el botón de modificar. Cambiar los valores que desee. Oprimir en el botón enviar.	
Resultado esperado: El sistema deberá mostrar la cantidad de dispositivos permitidos por persona y el tiempo de duración válido de una planilla.	
Resultado obtenido: El sistema muestra la cantidad de dispositivos permitidos por persona y el tiempo de duración válido de una planilla.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 50: Prueba de aceptación: Modificar configuración

Prueba de aceptación	
Código: HU4_P11	HU: Gestionar los tipos de dispositivos permitidos.

Nombre: Mostrar los tipos de dispositivos permitidos.
Descripción: Probar que el sistema permita a un usuario ver los tipos de dispositivos permitidos.
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para ver los tipos de dispositivos permitidos.
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Configuración.
Resultado esperado: El sistema deberá mostrar el nombre de los tipos de dispositivos permitidos.
Resultado obtenido: El sistema muestra el nombre de los tipos de dispositivos permitidos.
Evaluación de la respuesta: Prueba Satisfactoria.

Tabla 51: Prueba de aceptación: Mostrar los tipos de dispositivos permitidos

Prueba de aceptación	
Código: HU4_P12	HU: Gestionar los tipos de dispositivos permitidos.
Nombre: Modificar tipos de dispositivos permitidos.	
Descripción: Probar que el sistema permita a un usuario modificar el nombre de un tipo de dispositivo permitido.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para modificar el nombre de tipos de dispositivos permitidos.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Configuración. Seleccionar el dispositivo al cual desea hacerle la modificación. Cambiar el valor del nombre del tipo de dispositivo. Oprimir el botón de enviar.	
Resultado esperado: El sistema deberá modificar el nombre del tipo de dispositivos permitido seleccionado.	
Resultado obtenido: El sistema modifica el nombre del tipo de dispositivo permitido seleccionado.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 52: Prueba de aceptación: Modificar tipos de dispositivos permitidos

Prueba de aceptación	
Código: HU4_P13	HU: Gestionar los tipos de dispositivos permitidos.

Nombre: Insertar tipos de dispositivos permitidos.
Descripción: Probar que el sistema permita a un usuario insertar un tipo de dispositivo permitido.
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para insertar tipos de dispositivos permitidos.
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Configuración. Oprimir el botón insertar. Completar los campos. Oprimir el botón de enviar.
Resultado esperado: El sistema deberá insertar el tipo de dispositivos permitido.
Resultado obtenido: El sistema inserta el tipo de dispositivos permitido.
Evaluación de la respuesta: Prueba Satisfactoria.

Tabla 53: Prueba de aceptación: Insertar tipos de dispositivos permitidos

Prueba de aceptación	
Código: HU4_P14	HU: Gestionar los tipos de dispositivos permitidos.
Nombre: Eliminar tipos de dispositivos permitidos.	
Descripción: Probar que el sistema permita a un usuario eliminar uno o varios tipos de dispositivos permitidos.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para eliminar tipos de dispositivos permitidos.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Configuración. Seleccionar los tipos de dispositivos que desea eliminar. Oprimir el botón Eliminar.	
Resultado esperado: El sistema deberá eliminar los tipos de dispositivos permitidos seleccionados.	
Resultado obtenido: El sistema elimina los tipos de dispositivos permitidos seleccionados.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 54: Prueba de aceptación: Eliminar tipos de dispositivos permitidos

Prueba de aceptación

Código: HU5_P15	HU: Gestionar fabricantes de tarjetas de red y sus MACs.
Nombre: Comprobar validez de MAC.	
Descripción: Probar que el sistema permita a un usuario validar una MAC haciendo uso de la API http://api.macvendors.com/ .	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para comprobar validez de MAC.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Mac-Fabricante. Seleccionar las MAC que desea comprobar Oprimir el botón Comprobar.	
Resultado esperado: El sistema deberá comprobar las MACs seleccionadas a través de la API http://api.macvendors.com/ y modificará el valor del fabricante en la planilla relacionada con la MAC.	
Resultado obtenido: El sistema comprueba las MACs seleccionadas a través de la API http://api.macvendors.com/ y modifica el valor del fabricante en la planilla relacionada con la MAC.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 55: Prueba de aceptación: Comprobar validez de MAC

Prueba de aceptación	
Código: HU5_P16	HU: Gestionar fabricantes de tarjetas de red y sus MACs.
Nombre: Mostrar fabricantes de tarjetas de red y sus MACs.	
Descripción: Probar que el sistema permita a un usuario poder ver los fabricantes de tarjetas de red y sus MACs asignadas.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para ver fabricantes de tarjetas de red y sus MACs asignadas.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Mac-Fabricante.	
Resultado esperado: El sistema deberá mostrar el nombre del fabricante de tarjetas de red y la MAC asignada.	
Resultado obtenido: El sistema muestra el nombre del fabricante de tarjeta de red y la MAC asignada.	

Evaluación de la respuesta: Prueba Satisfactoria.

Tabla 56: Prueba de aceptación: Mostrar fabricantes de tarjetas de red

Prueba de aceptación	
Código: HU6_P17	HU: Gestionar marcas y modelos de los dispositivos permitidos.
Nombre: Mostrar marcas	
Descripción: Probar que el sistema permita a un usuario poder ver las marcas insertadas.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para ver las marcas insertadas.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Marca-Modelo.	
Resultado esperado: El sistema deberá mostrar el nombre de la marca y el nombre del dispositivo al que pertenece.	
Resultado obtenido: El sistema muestra el nombre de la marca y el nombre del dispositivo al que pertenece.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 57: Prueba de aceptación: Mostrar marcas

Prueba de aceptación	
Código: HU6_P18	HU: Gestionar marcas y modelos de los dispositivos permitidos.
Nombre: Modificar marcas	
Descripción: Probar que el sistema permita a un usuario poder modificar los valores de una marca determinada.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para modificar las marcas.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Marca-Modelo. Seleccionar una marca. Oprimir el botón Modificar. Modificar los valores. Oprimir el botón enviar.	

Resultado esperado: El sistema deberá modificar el nombre de la marca y el dispositivo al que pertenece.
Resultado obtenido: El sistema modifica el nombre de la marca y el dispositivo al que pertenece.
Evaluación de la respuesta: Prueba Satisfactoria.

Tabla 58: Prueba de aceptación: Modificar Marcas

Prueba de aceptación	
Código: HU6_P19	HU: Gestionar marcas y modelos de los dispositivos permitidos.
Nombre: Insertar marcas	
Descripción: Probar que el sistema permita a un usuario poder insertar una marca.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para insertar marcas.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Marca-Modelo. Oprimir el botón Insertar. Completar los campos. Oprimir el botón enviar.	
Resultado esperado: El sistema deberá insertar la marca en la base de datos.	
Resultado obtenido: El sistema inserta la marca en la base de datos.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 59: Prueba de aceptación: Insertar marcas

Prueba de aceptación	
Código: HU6_P20	HU: Gestionar marcas y modelos de los dispositivos permitidos.
Nombre: Eliminar marcas.	
Descripción: Probar que el sistema permita a un usuario poder eliminar marcas.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para eliminar marcas.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Marca-Modelo. Seleccionar una o varias marcas. Oprimir el botón eliminar.	

Resultado esperado: El sistema deberá eliminar las marcas seleccionadas.
Resultado obtenido: El sistema elimina las marcas seleccionadas.
Evaluación de la respuesta: Prueba Satisfactoria.

Tabla 60: Prueba de aceptación: Eliminar marcas

Prueba de aceptación	
Código: HU6_P21	HU: Gestionar marcas y modelos de los dispositivos permitidos.
Nombre: Mostrar modelos	
Descripción: Probar que el sistema permita a un usuario poder ver los modelos insertados.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para ver los modelos insertados.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Marca-Modelo.	
Resultado esperado: El sistema deberá mostrar el nombre del modelo y el nombre de la marca a la que pertenece.	
Resultado obtenido: El sistema muestra el nombre del modelo y el nombre de la marca a la que pertenece.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 61: Prueba de aceptación: Mostrar modelos

Prueba de aceptación	
Código: HU6_P22	HU: Gestionar marcas y modelos de los dispositivos permitidos.
Nombre: Modificar modelos	
Descripción: Probar que el sistema permita a un usuario poder modificar los valores de un modelo determinado.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para modificar los modelos.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Marca-Modelo. Seleccionar un modelo. Oprimir el botón Modificar. Modificar los valores. Oprimir el botón enviar.	

Resultado esperado: El sistema deberá modificar el nombre del modelo y la marca a la que pertenece.
Resultado obtenido: El sistema modifica el nombre del modelo y la marca a la que pertenece.
Evaluación de la respuesta: Prueba Satisfactoria.

Tabla 62: Prueba de aceptación: Modificar modelos

Prueba de aceptación	
Código: HU6_P23	HU: Gestionar marcas y modelos de los dispositivos permitidos.
Nombre: Insertar modelos.	
Descripción: Probar que el sistema permita a un usuario poder insertar un modelo.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para insertar modelos.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Marca-Modelo. Oprimir el botón Insertar. Completar los campos. Oprimir el botón enviar.	
Resultado esperado: El sistema deberá insertar el modelo en la base de datos.	
Resultado obtenido: El sistema inserta el modelo en la base de datos.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 63: Prueba de aceptación: Insertar modelos

Prueba de aceptación	
Código: HU6_P24	HU: Gestionar marcas y modelos de los dispositivos permitidos.
Nombre: Eliminar modelos.	
Descripción: Probar que el sistema permita a un usuario poder eliminar modelos.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para eliminar modelos.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Marca-Modelo. Seleccionar una o varios modelos. Oprimir el botón eliminar.	
Resultado esperado: El sistema deberá eliminar los modelos seleccionados.	

Resultado obtenido: El sistema elimina los modelos seleccionados.
Evaluación de la respuesta: Prueba Satisfactoria.

Tabla 64: Prueba de aceptación: Eliminar modelos

Prueba de aceptación	
Código: HU6_P25	HU: Generar reportes.
Nombre: Mostrar reportes.	
Descripción: Probar que el sistema permita a un usuario poder ver reportes.	
Condiciones de ejecución: El usuario debe estar previamente autenticado y tener permisos para ver reportes.	
Entradas/Pasos de ejecución: Autenticarse en el sistema. Oprimir el botón Reportes.	
Resultado esperado: El sistema deberá mostrar los reportes de estadísticas.	
Resultado obtenido: El sistema muestra los reportes de estadísticas.	
Evaluación de la respuesta: Prueba Satisfactoria.	

Tabla 65: Prueba de aceptación: Mostrar reportes

Después de haber aplicado las pruebas de aceptación se alcanzaron los siguientes resultados en cada una de las iteraciones:

- ✓ En la primera iteración se identificaron un total de 3 no conformidades las cuales quedaron resueltas.
- ✓ En la segunda iteración se identificaron un total de 1 no conformidad la cual fue resuelta de forma satisfactoria.
- ✓ En la tercera iteración no se identificaron no conformidades cumpliendo con las funcionalidades definidas y así alcanzar el resultado satisfactorio.

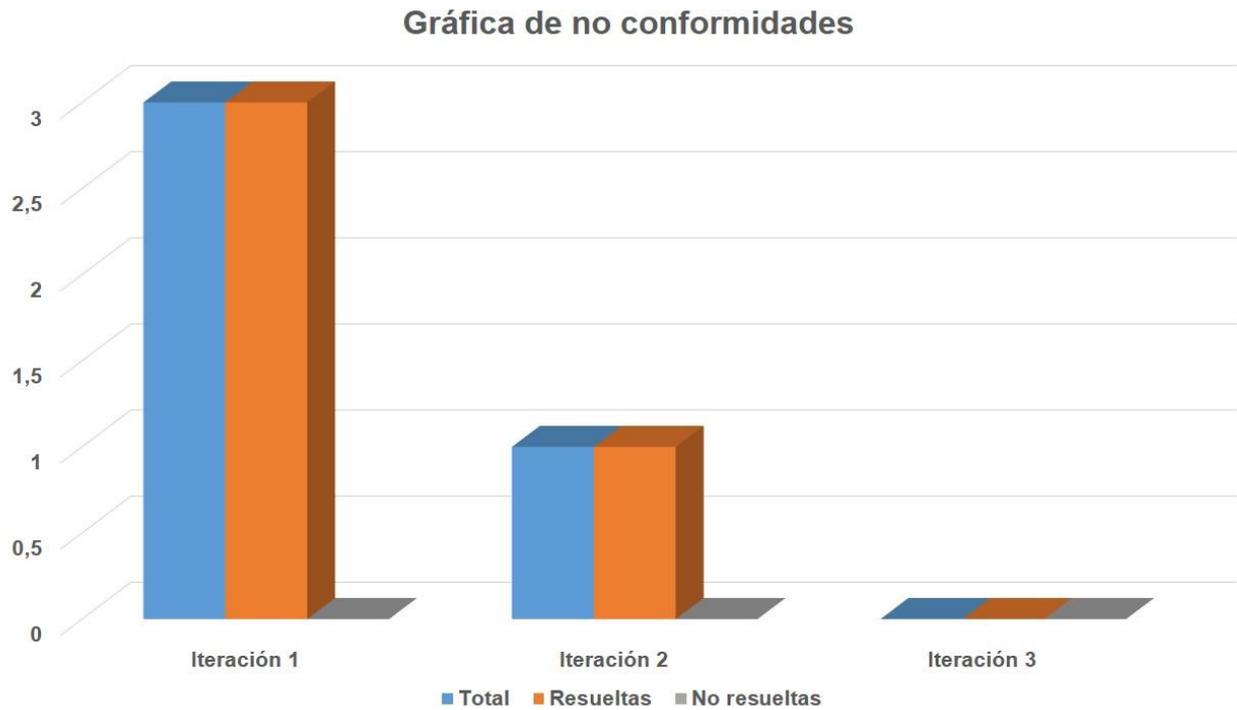


Figura 8: Gráfica de los resultados obtenidos de aplicar pruebas de aceptación

5.2 Conclusiones del capítulo

En este capítulo se realizaron las pruebas unitarias y las pruebas de aceptación o funcionales. Las pruebas unitarias sirvieron para asegurar que los componentes de la aplicación producen una salida correcta para una determinada entrada. Por otra parte las pruebas de aceptación se realizaron con el objetivo de garantizar que los requerimientos han sido cumplidos y que el sistema es aceptable por el cliente.

CONCLUSIONES GENERALES

Los resultados obtenidos al concluir esta investigación, aportan la creación de un sistema para la autorización y control de dispositivos inalámbricos que acceden a la red inalámbrica en la Universidad de las Ciencias Informáticas, que permite tener un mayor control sobre los dispositivos que hacen uso de su sistema de red. La aplicación fue desarrollada siguiendo los principios de la metodología XP, lo que permitió realizar un desarrollo ágil y dentro de los plazos previstos con la total conformidad del cliente. Los artefactos obtenidos, sirven de base para una futura ampliación del sistema, en vista de continuar incrementando sus funcionalidades para seguir adaptándolo a las necesidades reales del entorno donde se utilizará. Todo el trabajo realizado posibilitó darle cumplimiento al objetivo general de la investigación.

RECOMENDACIONES

A partir del trabajo realizado se recomienda:

- ✓ Procesar los logs obtenidos de los Puntos de Acceso desplegados en la universidad para obtener un mayor conjunto de datos, poder obtener mayor cantidad de reportes y permitir el control de acceso.

REFERENCIAS BIBLIOGRÁFICAS

1. [En línea] [Citado el: 3 de mayo de 2016.] <http://conceptodefinicion.de/procedimiento/>.
2. [En línea] [Citado el: 2 de mayo de 2016.] <http://es.thefreedictionary.com/autorizar>.
3. [En línea] [Citado el: 2 de mayo de 2016.] <http://es.thefreedictionary.com/control>.
4. [En línea] [Citado el: 2 de mayo de 2016.] <https://mistareasdecomputacion.wordpress.com/2011/11/13/%C2%BFque-es-un-dispositivo-inalambrico/>.
5. PacketFence. [En línea] [Citado el: 2 de mayo de 2016.] <http://packetfence.org/>.
6. openNAC. [En línea] [Citado el: 1 de mayo de 2016.] <http://www.opennac.org/opennac/en.html>.
7. [En línea] [Citado el: 4 de mayo de 2016.] http://www.cisco.com/c/en/us/products/security/nac-appliance-clean-access/index.html?referring_site=bodynav.
8. [En línea] [Citado el: 3 de mayo de 2016.] <http://extremenetworks.com/product/extreme-access-control/>.
9. [En línea] [Citado el: 23 de abril de 2016.] <http://www.um.es/docencia/barzana/IAGP/lagp2.html>.
10. php. [En línea] [Citado el: 28 de abril de 2016.] <http://php.net/>.
11. [En línea] [Citado el: 22 de abril de 2016.] <http://www.w3c.es/Divulgacion/GuiasBreves/HojasEstilo>.
12. [En línea] [Citado el: 3 de mayo de 2016.] <https://developer.mozilla.org/es/docs/Web/JavaScript>.
13. acerca de HTML. [En línea] [Citado el: 20 de abril de 2016.] <http://www.acercadehtml.com/manual-html/que-es-html.html>.
14. Twig. [En línea] [Citado el: 21 de abril de 2016.] <http://twig.sensiolabs.org/>.
15. symfony.es. [En línea] [Citado el: 26 de abril de 2016.] symfony.es/.
16. Dojo. [En línea] [Citado el: 25 de Abril de 2016.] <http://dojofoundation.org/projects/dojo>.
17. PostgreSQL-es. [En línea] [Citado el: 26 de abril de 2016.] http://www.postgresql.org.es/sobre_postgresql.
18. [En línea] [Citado el: 3 de mayo de 2016.] <http://oness.sourceforge.net/proyecto/html/ch05s02.html>.

19. Izaurralde, María Paula. [En línea] [Citado el: 24 de Abril de 2016.] www.institucional.frc.utn.edu.ar/sistemas/lidicalso/pub/file/Tesis/Anteproyecto_Requerimientos_en_Metodologías_Agiles.pdf.
20. Pressman, Roger S. *Ingeniería del software*. 2002.
21. Academia. [En línea] [Citado el: 4 de mayo de 2016.] http://www.academia.edu/8991103/Patrones_de_dise%C3%B1o_de_software.
22. Abraham Silberschatz, Henry F. Korth, S. Sudarshan. *FUNDAMENTOS DE BASES DE DATOS*. 2002.
23. Tobón, Luis Miguel Echeverry y Delgado Carmona, Luz Elena. *Caso práctico de la metodología ágil XP al desarrollo de software*. 2007.
24. Eguiluz, Javier. *Desarrollo web ágil con Symfony 2*. 2013.
25. Potencier, Fabien y Zaninotto, Francois . *Symfony la guía definitiva*. 2007.
26. Garcia M, Saul. *Django, la guía definitiva*. 2015.

BIBLIOGRAFÍA

1. [En línea] [Citado el: 3 de mayo de 2016.] <http://conceptodefinicion.de/procedimiento/>.
2. [En línea] [Citado el: 2 de mayo de 2016.] <http://es.thefreedictionary.com/autorizar>.
3. [En línea] [Citado el: 2 de mayo de 2016.] <http://es.thefreedictionary.com/control>.
4. [En línea] [Citado el: 2 de mayo de 2016.] <https://mistareasdecomputacion.wordpress.com/2011/11/13/%C2%BFque-es-un-dispositivo-inalambrico/>.
5. PacketFence. [En línea] [Citado el: 2 de mayo de 2016.] <http://packetfence.org/>.
6. openNAC. [En línea] [Citado el: 1 de mayo de 2016.] <http://www.opennac.org/opennac/en.html>.
7. [En línea] [Citado el: 4 de mayo de 2016.] http://www.cisco.com/c/en/us/products/security/nac-appliance-clean-access/index.html?referring_site=bodynav.
8. [En línea] [Citado el: 3 de mayo de 2016.] <http://extremenetworks.com/product/extreme-access-control/>.
9. [En línea] [Citado el: 23 de abril de 2016.] <http://www.um.es/docencia/barzana/IAGP/lagp2.html>.
10. php. [En línea] [Citado el: 28 de abril de 2016.] <http://php.net/>.
11. [En línea] [Citado el: 22 de abril de 2016.] <http://www.w3c.es/Divulgacion/GuiasBreves/HojasEstilo>.
12. [En línea] [Citado el: 3 de mayo de 2016.] <https://developer.mozilla.org/es/docs/Web/JavaScript>.
13. acerca de HTML. [En línea] [Citado el: 20 de abril de 2016.] <http://www.acercadehtml.com/manual-html/que-es-html.html>.
14. Twig. [En línea] [Citado el: 21 de abril de 2016.] <http://twig.sensiolabs.org/>.
15. symfony.es. [En línea] [Citado el: 26 de abril de 2016.] symfony.es/.
16. Dojo. [En línea] [Citado el: 25 de Abril de 2016.] <http://dojofoundation.org/projects/dojo>.
17. PostgreSQL-es. [En línea] [Citado el: 26 de abril de 2016.] http://www.postgresql.org.es/sobre_postgresql.
18. [En línea] [Citado el: 3 de mayo de 2016.] <http://oness.sourceforge.net/proyecto/html/ch05s02.html>.

19. Izaurralde, María Paula. [En línea] [Citado el: 24 de Abril de 2016.] www.institucional.frc.utn.edu.ar/sistemas/lidicalso/pub/file/Tesis/Anteproyecto_Requerimientos_en_Metodologías_Agiles.pdf.
20. Pressman, Roger S. *Ingeniería del software*. 2002.
21. Academia. [En línea] [Citado el: 4 de mayo de 2016.] http://www.academia.edu/8991103/Patrones_de_dise%C3%B1o_de_software.
22. Abraham Silberschatz, Henry F. Korth, S. Sudarshan. *FUNDAMENTOS DE BASES DE DATOS*. 2002.
23. Tobón, Luis Miguel Echeverry y Delgado Carmona, Luz Elena. *Caso práctico de la metodología ágil XP al desarrollo de software*. 2007.
24. Eguiluz, Javier. *Desarrollo web ágil con Symfony 2*. 2013.
25. Potencier, Fabien y Zaninotto, Francois . *Symfony la guía definitiva*. 2007.
26. Garcia M, Saul. *Django, la guía definitiva*. 2015.
27. Dojo. [En línea] <https://dojotoolkit.org/>.
28. Vesterinen, Konsta y Wage, Jonathan. *Doctrine Manual*. 2008.
29. Mateu, Carlos. *Desarrollo de aplicaciones web*. 2004.
30. Pérez, Javier Eguíluz. *Introducción a CSS*. 2009.
31. Ortega, Ivan Sánchez. *Curso de PHP 5*. 2005.

ANEXOS

Anexo 1: Tareas de ingeniería de la primera iteración.

Tarea de ingeniería	
Nombre: Listar planillas	
HU: Procesar planillas de solicitud	Puntos estimados: 0.4
Fecha de inicio: 14/03/2016	Fecha de fin: 15/03/2016
Descripción: Un usuario puede ver a través de una tabla el tipo de dispositivo, la marca, el modelo, la mac, el número de serie y el estado en que se encuentran las planillas que ha solicitado. Estos datos deberá adquirírselos de la base de datos.	

Tabla 66: Tarea de ingeniería: Listar planillas

Tarea de ingeniería	
Nombre: Cancelar planilla	
HU: Procesar planillas de solicitud	Puntos estimados: 0.2
Fecha de inicio: 18/03/2016	Fecha de fin: 18/03/2016
Descripción: Un usuario puede cancelar sus planillas y el sistema deberá pedirle confirmación antes de cancelarla. Si la confirmación es positiva el sistema debe eliminar la planilla de la base de datos.	

Tabla 67: Tarea de Ingeniería: Cancelar planilla

Tarea de ingeniería	
Nombre: Ver planilla en formato PDF	
HU: Procesar planillas de solicitud	Puntos estimados: 0.6
Fecha de inicio: 21/03/2016	Fecha de fin: 23/03/2016
Descripción: Un usuario que tenga permiso de ver las planillas en formato PDF podrá listar todas las planillas, seleccionar la que desea y deberá presionar un botón para ver la planilla en ese formato.	

Tabla 68: Tarea de Ingeniería: Ver planillas en formato PDF

Tarea de ingeniería	
Nombre: Firmar como directivo	

HU: Procesar planillas de solicitud	Puntos estimados: 0.4
Fecha de inicio: 24/03/2016	Fecha de fin: 25/03/2016
Descripción: Un usuario que tenga permisos de firma puede ver las planillas que pertenezcan a un área sobre la cual él tiene permiso de firma. Una vez que el sistema le muestre todos los datos de las planillas (usuario, tipo de dispositivo, marca, modelo, mac, número de serie, estado) podrá aprobar o rechazar las que seleccione. Si el usuario aprueba la planilla se modificará el valor del estado en que se encuentra de pendiente a aprobada. Si el usuario rechaza la planilla se modificará el valor del estado en que se encuentra de pendiente a rechazada.	

Tabla 69: Tarea de Ingeniería: Firmar como directivo

Tarea de ingeniería	
Nombre: Buscar información de planillas	
HU: Procesar planillas de solicitud	Puntos estimados: 0.6
Fecha de inicio: 28/03/2016	Fecha de fin: 30/03/2016
Descripción: Un usuario que tenga permiso de buscar información sobre las planillas podrá realizar búsquedas sobre estas. El usuario deberá presionar un botón para aplicar un filtro y deberá proporcionarle al sistema los campos y los valores sobre los cuales quiere realizarlo. El sistema deberá mostrarle en una tabla con todos los datos de las planillas que haya devuelto la consulta sobre la base de datos.	

Tabla 70: Tarea de Ingeniería: Buscar información de planillas

Tarea de ingeniería	
Nombre: Exportar información de planillas	
HU: Procesar planillas de solicitud	Puntos estimados: 0.4
Fecha de inicio: 31/03/2016	Fecha de fin: 1/04/2016
Descripción: Un usuario que tenga permiso podrá exportar a formato csv alguna búsqueda realizada anteriormente. El usuario deberá presionar un botón para poder exportar.	

Tabla 71: Tarea de Ingeniería: Exportar información

Anexo 2: Tareas de ingeniería de la segunda iteración.

Tarea de ingeniería	
Nombre: Mostrar permisos de firma	
HU: Gestionar permisos de firmas	Puntos estimados: 0.6
Fecha de inicio: 11/04/2016	Fecha de fin: 13/04/2016
Descripción: Un usuario que tenga permiso puede ver mediante una tabla los permisos de firma que están insertados en la base de datos. Se mostrará una tabla con una columna llamada usuario y otra columna llamada área significando esto que un determinado usuario tiene permiso de firma sobre una determinada área.	

Tabla 72: Tarea de Ingeniería: Mostrar permisos de firma

Tarea de ingeniería	
Nombre: Eliminar permisos de firma	
HU: Gestionar permisos de firmas	Puntos estimados: 0.4
Fecha de inicio: 14/04/2016	Fecha de fin: 15/04/2016
Descripción: Un usuario que tenga permiso puede eliminar alguna relación entre un usuario y un área significando esto que ese usuario no tendrá permiso de firma sobre esa área. El usuario deberá seleccionar la(s) relaciones que desea eliminar y presionará un botón para eliminar dicha relación. Antes de realizar esta operación el sistema deberá pedir confirmación.	

Tabla 73: Tarea de Ingeniería Eliminar permisos de firma

Anexo 3: Tareas de ingeniería de la tercera iteración.

Tarea de ingeniería	
Nombre: Modificar configuración	
HU: Gestionar configuraciones	Puntos estimados: 0.1
Fecha de inicio: 18/04/2016	Fecha de fin: 18/04/2016
Descripción: Un usuario que tenga permiso puede modificar los valores de cantidad de dispositivos permitidos por persona y el tiempo de validez de una planilla de solicitud.	

Tabla 74: Tarea de Ingeniería: Modificar configuración

Tarea de ingeniería	
Nombre: Mostrar tipos de dispositivos permitidos	
HU: Gestionar los tipos de dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 19/04/2016	Fecha de fin: 19/04/2016
Descripción: Un usuario que tenga permiso puede ver mediante una tabla el nombre de los tipos de dispositivos permitidos insertados en la base de datos.	

Tabla 75: Tarea de Ingeniería: Mostrar tipos de dispositivos permitidos

Tarea de ingeniería	
Nombre: Modificar tipos de dispositivos permitidos	
HU: Gestionar los tipos de dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 19/04/2016	Fecha de fin: 19/04/2016
Descripción: Un usuario que tenga permiso puede modificar el nombre de los tipos de dispositivos permitidos insertados en la base de datos.	

Tabla 76: Tarea de Ingeniería: Modificar tipos de dispositivos permitidos

Tarea de ingeniería	
Nombre: Insertar tipos de dispositivos permitidos	
HU: Gestionar los tipos de dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 20/04/2016	Fecha de fin: 20/04/2016

Descripción: Un usuario que tenga permiso puede insertar un tipo de dispositivo permitido mediante un formulario al cual le deberá proporcionar el nombre.

Tabla 77: Tarea de Ingeniería: Insertar tipos de dispositivos permitidos

Tarea de ingeniería	
Nombre: Eliminar tipos de dispositivos permitidos	
HU: Gestionar los tipos de dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 20/04/2016	Fecha de fin: 20/04/2016
Descripción: Un usuario que tenga permiso puede eliminar un tipo de dispositivo permitido que esté insertado en la base de datos. Antes de eliminar el sistema deberá pedirle confirmación y de ser positiva se eliminará el tipo de dispositivo seleccionado.	

Tabla 78: Tarea de Ingeniería: Eliminar tipos de dispositivos permitidos

Tarea de ingeniería	
Nombre: Comprobar validez de MAC	
HU: Gestionar fabricantes de tarjetas de red y sus MACs.	Puntos estimados: 0.5
Fecha de inicio: 21/04/2016	Fecha de fin: 22/04/2016
Descripción: Un usuario que tenga permiso podrá obtener una lista de las planillas que sus MAC no han sido comprobadas a través de la base de datos del sistema. Tendrá la opción de seleccionar algunas de esas planillas y comprobar si la MAC es válida, esto se realizará a través de la API http://api.macvendors.com/ . Una vez comprobada que una MAC es válida se insertará su fabricante en la base de datos del sistema.	

Tabla 79: Tarea de Ingeniería: Comprobar Validez de MAC

Tarea de ingeniería	
Nombre: Mostrar fabricantes de tarjetas de red y sus MACs.	
HU: Gestionar fabricantes de tarjetas de red y sus MACs.	Puntos estimados: 0.1
Fecha de inicio: 25/04/2016	Fecha de fin: 25/04/2016

Descripción: Un usuario que tenga permiso puede ver mediante una tabla los fabricantes de tarjetas de red y sus MACs asociadas. Esta información deberá obtenerla de la base de datos.

Tabla 80: Tarea de Ingeniería: Mostrar fabricantes de tarjetas de red y sus MACs

Tarea de ingeniería	
Nombre: Mostar Marcas	
HU: Gestionar marcas y modelos de los dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 25/04/2016	Fecha de fin: 25/04/2016
Descripción: Un usuario que tenga permiso puede ver mediante una tabla el nombre de las marcas y el nombre del tipo de dispositivos al que pertenece. Esta información deberá obtenerla de la base de datos.	

Tabla 81: Tarea de Ingeniería: Mostrar Marcas

Tarea de ingeniería	
Nombre: Modificar Marcas	
HU: Gestionar marcas y modelos de los dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 26/04/2016	Fecha de fin: 26/04/2016
Descripción: Un usuario que tenga permiso puede modificar el nombre de las marcas asociadas a los tipos de dispositivos insertados. El usuario debe seleccionar la marca que desea modificar y el sistema le mostrará un formulario para que modifique los valores. Una vez que se realicen los cambios se deberán modificar en la base de datos.	

Tabla 82: Tarea de Ingeniería: Modificar Marcas

Tarea de ingeniería	
Nombre: Insertar Marcas	
HU: Gestionar marcas y modelos de los dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 26/04/2016	Fecha de fin: 26/04/2016
Descripción: Un usuario que tenga permiso puede insertar marcas asociadas a los tipos de dispositivos permitidos insertados en la base de datos. Esto se realizará a través de un	

formulario que se deberá llenar con el nombre de la marca y el tipo de dispositivo al que pertenece.

Tabla 83: Tarea de Ingeniería: Insertar Marcas

Tarea de ingeniería	
Nombre: Eliminar Marcas	
HU: Gestionar marcas y modelos de los dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 27/04/2016	Fecha de fin: 27/04/2016
Descripción: Un usuario que tenga permiso puede eliminar las marcas que han sido insertadas en la base de datos. El usuario deberá seleccionar la marca que desea eliminar y presionará un botón. El sistema deberá pedirle confirmación antes de eliminar. Si la respuesta es afirmativa se deberá eliminar de la base de datos.	

Tabla 84: Tarea de Ingeniería: Eliminar Marcas

Tarea de ingeniería	
Nombre: Mostrar Modelos	
HU: Gestionar marcas y modelos de los dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 27/04/2016	Fecha de fin: 27/04/2016
Descripción: Un usuario que tenga permiso puede ver mediante una tabla el nombre de los modelos y el nombre de la marca a la que está asociada. Esta información deberá obtenerse de la base de datos.	

Tabla 85: Tarea de Ingeniería: Mostrar Modelos

Tarea de ingeniería	
Nombre: Modificar Modelos	
HU: Gestionar marcas y modelos de los dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 28/04/2016	Fecha de fin: 28/04/2016
Descripción: Un usuario que tenga permiso puede modificar el nombre de los modelos asociados a las marcas insertadas. El usuario deberá proporcionarle al sistema el nuevo	

nombre del modelo después de haberlo seleccionado y haber apretado el botón de modificar.

Tabla 86: Tarea de Ingeniería: Modificar Modelos

Tarea de ingeniería	
Nombre: Insertar Modelos	
HU: Gestionar marcas y modelos de los dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 28/04/2016	Fecha de fin: 28/04/2016
Descripción: Un usuario que tenga permiso puede insertar modelos. Esto se realizará a través de un formulario que se llenará con el nombre del modelo y el nombre de la marca a la que pertenece.	

Tabla 87: Tarea de Ingeniería: Insertar Modelos

Tarea de ingeniería	
Nombre: Eliminar Modelos	
HU: Gestionar marcas y modelos de los dispositivos permitidos	Puntos estimados: 0.1
Fecha de inicio: 29/04/2016	Fecha de fin: 29/04/2016
Descripción: Un usuario que tenga permiso puede eliminar modelos. El usuario deberá seleccionar el o los modelos que desea eliminar y deberá presionar un botón para eliminar. El sistema deberá pedirle confirmación y de ser positiva deberá eliminar el modelo de la base de datos.	

Tabla 88: Tarea de Ingeniería: Eliminar Modelos

Tarea de ingeniería	
Nombre: Mostrar Reportes	
HU: Generar Reportes	Puntos estimados: 1
Fecha de inicio: 2/05/2016	Fecha de fin: 6/05/2016
Descripción: Un usuario que tenga permiso de ver algún reporte de estadísticas el sistema deberá mostrárselo a través de tablas. Deberá mostrarse en una tabla la cantidad histórica de planillas aprobadas y la cantidad de planillas aprobadas en el año.	

Deberá mostrarse la cantidad histórica de personas con al menos una solicitud aprobada y la cantidad de personas con al menos una solicitud aprobada en el año. Deberá mostrarse en una tabla la cantidad histórica de solicitudes aprobadas por área y la cantidad de solicitudes aprobadas por área en el año. Deberá mostrarse la cantidad por cada fabricante de tarjetas de red en la UCI. Deberá mostrarse la cantidad por cada fabricante de tarjetas de red en la base de datos.

Tabla 89: Tarea de Ingeniería: Mostrar Reportes