TT-CIS-XA-001

UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"Disminución de la Suplantación de Identidad dentro de una Plataforma Virtual de Aprendizaje mediante la Autenticación por Huella Dactilar"

Tesis Previa a la obtención del Título de Ingeniero en Sistemas

Autores:

- *Bravo – Brito, Darío-Ignacio.*
- *Troya - Iriarte, María–Magdalena.*

Director:

Ing. Conde-Zhingre, Lorena – Elizabeth, Mg. Sc.

LOJA – ECUADOR

2015

Certificación de director

27 de febrero de 2015

Ingeniera Lorena Elizabeth Conde Zhingre, Mg. Sc.

DIRECTOR DE TESIS

CERTIFICA:

Haber dirigido, revisado y corregido el trabajo de tesis **"Disminución de la suplantación de Identidad dentro de una Plataforma Virtual de Aprendizaje mediante la Autenticación por Huella Dactilar"**, realizado por los egresados María Magdalena Troya Iriarte y Darío Ignacio Bravo Brito, previo a la obtención del título de INGENIERO EN SISTEMAS.

En vista de que el mismo reúne los requisitos necesarios autorizo su presentación y defensa ante el tribunal que se designe para el efecto.

Atentamente;

Ing. Lorena Elizabeth Conde Zhingre, Mg. Sc.

Autoría

Nosotros, **MARÍA MAGDALENA TROYA IRIARTE** y **DARÍO IGNACIO BRAVO BRITO,** declaran ser autores del presente trabajo de tesis y eximimos expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales por el contenido de la misma.

Adicionalmente aceptan y autorizan a la Universidad Nacional de Loja, la publicación nuestro trabajo de titulación en el Repositorio Institucional – Biblioteca Virtual.

Firma: ……

Autor: María Magdalena Troya Iriarte

Cédula: 1104615966

Fecha: 30-04-2015

Firma: ……

Autor: Darío Ignacio Bravo Brito

Cédula: 1105032161

Carta De Autorización De Tesis Por Parte De Los Autores, Para La Consulta, Reproducción Parcial O Total Y Publicación Electrónica Del Texto Completo.

Nosotros, **MARÍA MAGDALENA TROYA IRIARTE** y **DARÍO IGNACIO BRAVO BRITO,** declaran ser autores de la tesis titulada: **"DISMINUCIÓN DE LA SUPLANTACIÓN DE IDENTIDAD DENTRO DE UNA PLATAFORMA VIRTUAL DE APRENDIZAJE MEDIANTE LA AUTENTICACIÓN POR HUELLA DACTILAR"**, como requisito para optar al grado de: **INGENIERO EN SISTEMAS;** autorizamos al Sistema Bibliotecario de la Universidad Nacional de Loja, para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Por constancia de esta autorización, en la ciudad de Loja, a los treinta días del mes de abril del dos mil quince.

Firma:…….

Autor: María Magdalena Troya Iriarte.

Cédula: 1104615966.

Dirección: Cdla. Pio Jaramillo Alvarado.

Teléfono: 2583263 **Celular:** 0980450309

Correo Electrónico: mmtroi@unl.edu.ec

Firma:…….

Autor: Darío Ignacio Bravo Brito**.**

Cédula: 1104615966.

Dirección: San Vicente Alto.

Teléfono: 2713343 **Celular:** 0990712695.

Correo Electrónico: dibravob@unl.edu.ec

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Lorena Elizabeth Conde Zhingre., Mg. Sc.

Tribunal de Grado: Ing. Alex Vinicio Padilla Encalada., Mg. Sc.
Ing. Waldemar Victorino Espinoza Tituana., Mg. Sc.
Ing. Carlos Miguel Jaramillo Castro., Mg. Sc.

Agradecimiento

Antes que nada quisiera agradecerle a Dios por darme todas las fuerzas y las ganas de seguir adelante.

A mis padres quienes se constituyeron en un pilar fundamental en mi vida apoyándome en todo momento y sobre todo porque confiaron siempre en mí convirtiéndose en mi inspiración a lo largo de todos mis estudios.

A mis compañeros que fueron parte fundamental de este logro apoyándonos en cada momento.

A la Universidad Nacional de Loja por abrirme las puertas y permitirme llevar a cabo la culminación de mi Carrera.

A todos los docentes que formaron parte de mis estudios, quienes compartieron sus conocimientos y apoyo para cumplir con cada tarea asignada.

Darío Ignacio Bravo Brito

Agradezco a Dios por haberme permitido culminar el presente Trabajo de Titulación con éxito, a todos los Docentes que con su formación profesional y su gran experiencia me inculcaron el conocimiento y el deseo de superación.

A mi padre por ser guía y pilar fundamental durante toda mi etapa académica, a mis hermanos por su paciencia y los momentos compartidos.

Finalmente, gracias a todos mis compañeros de aula, y a todos aquellos que de una u otra manera hicieron posible la culminación de esta magnífica etapa.

María Magdalena Troya Iriarte

Dedicatoria

A Dios por permitirme llegar a este momento muy especial en mi vida y darme las fuerzas para superar cada uno de los obstáculos y dificultades presentadas durante el transcurro de la Carrera Universitaria.

A mis padres que me han brindado apoyo incondicional, agradecido de corazón por cada momento, por sus consejos que me han sabido guiar para poder culminar mi carrera Profesional.

A toda mi familia que me ha brindado el apoyo para seguir siempre adelante y nunca desmayar.

Darío Ignacio Bravo Brito

Dedico este Proyecto Fin de Carrera primeramente a Dios por regalarme la vida, y por estar siempre a lado mío dándome las fuerzas necesarias para superar los momentos difíciles y haberme permitido llegar hasta esta etapa de mi vida.

A mi padre por el apoyo brindado en cada momento, por su sacrificio y esfuerzo que me inspiran a ser mejor

A mi familia por creer siempre en mí, por su apoyo y estar conmigo en las buenas y en las malas, por sus consejos de superación han logrado motivarme para seguir adelante.

María Magdalena Troya Iriarte

a. Título

Disminución de la suplantación de Identidad dentro de una Plataforma Virtual de Aprendizaje mediante la Autenticación por Huella Dactilar

b. Resumen

El presente Proyecto de Fin de Carrera presenta la integración de un sistema biométrico de huella dactilar a una plataforma virtual de aprendizaje (Moodle), con la finalidad de minimizar la suplantación de identidad de los usuarios, especialmente dentro de los procesos de evaluación, garantizando que el usuario sea quien dice ser e incrementando el nivel de seguridad al acceso a la plataforma.

En la primera fase del Proyecto se realiza un estudio y comparación de los diferentes sistemas biométricos con el fin de seleccionar uno que se adapte de mejor manera a la plataforma Moodle, así mismo se realiza un estudio de casos de éxito con la finalidad de conocer los diversos ambientes de una educación a distancia y las desventajas que tienen estos en cuanto a seguridad se refiere.

En la segunda fase, se configura la plataforma Moodle, se detalla el desarrollo del sistema de verificación de identidad utilizando el sistema biométrico de huella dactilar, se identifica las herramientas software utilizadas y como un siguiente paso se realiza la integración del método de verificación con la mencionada plataforma, con la utilización de applets y realizando configuraciones en el código interno de la plataforma.

En la tercera fase, se emplea técnicas que permitan proteger los datos confidenciales que viajan a través de la red, haciendo uso del protocolo HTTPS, el RECAPTCHA que permite verificar que personas no autorizadas o con una entidad falsa tengan ingreso y saturen el servidor al contar con usuarios falsos, plantillas encriptadas de la huella, que permiten que la información no sea alterada, modificada o manipulada por personas no autorizadas para beneficio de los mismos.

En la cuarta fase, se pone en marcha el proyecto en modo de prueba con el fin de detectar posibles errores tantos técnicos como lógicos, además se plantea soluciones a los errores y problemas encontrados en cuanto al acceso a la plataforma y al módulo de evaluaciones. Finalmente se obtiene como resultado el funcionamiento del sistema de autenticación biométrica integrado a la plataforma.

De la misma manera se presentan las conclusiones y recomendaciones que se han obtenido en base a los resultados obtenidos en el desarrollo de este proyecto.

Summary

This Thesis Project presents the integration of a biometric fingerprint system to a virtual learning platform (Moodle), in order to minimize spoofing of users, especially within the evaluation process, ensuring that the user is who they say they are and increasing the security level access to the platform.

In the first phase of the project a study and comparison of different biometric systems is done in order to select one that fits better to the Moodle platform, likewise a successful case study is performed in order to meet the different environments of distance education and the disadvantages in terms of security.

In the second phase, the platform Moodle is configured, the development of the identity verification system is detailed using biometric fingerprint system, the software tools used are identified and as a next step the integration method of verification is done with the platform mention above, this is done with the use of applets and making settings in the internal code of the platform.

In the third phase, techniques to protect sensitive data traveling over the network, using the HTTPS protocol, the ReCaptcha verifies that unauthorized people or false entity have access and saturate the server with fake users, encrypted fingerprint templates, which allow the information is not altered, modified or tampered with by unauthorized persons to benefit them.

In the fourth phase, the project is launched in test mode in order to detect both technical and logical possible errors, in addition, solutions to errors and problems encountered in the access to the platform and to the assessments module are proposed. Finally, we obtain as result the operation of the biometric authentication system integrated to the platform.

Likewise the conclusions and recommendations that have been obtained based on the results obtained in the development of this project are presented.

Índice de Contenidos

Índice General

Índice de Figuras

Índice de Tablas

c. Introducción

En el mundo digital actual, la autenticación personal se ha tornado en una de las actividades importantes en la interfaz computacional y humana. Es así que uno de los métodos de autenticación, se ha convertido en la herramienta más eficaz para la identificación de personas, usando características únicas de cada individuo.

La implementación de sistemas biométricos ha permitido automatizar los procesos de reconocimiento de identidad, de manera que pueden ser aplicados a mejorar los procesos de seguridad, siendo así la biometría se ha convertido en un elemento clave en cuanto a técnicas de identificación.

Por tal razón nuestra propuesta consiste en integrar un sistema biométrico de huella dactilar a una plataforma virtual de aprendizaje (Moodle), con la finalidad de minimizar la suplantación de identidad de los usuarios, especialmente dentro de los procesos de evaluación, realizados dentro de las mismas, garantizando que el usuario es quien dice ser.

Esta aplicación de la biometría permite satisfacer la necesidad de mejorar los sistemas actuales de enseñanza de las plataformas virtuales de aprendizaje, haciendo mucho más seguro el acceso y control de los usuarios dentro del mismo, además de garantizar la fiabilidad de los cursos dictados por cada uno de los docentes al tener un control dentro de los procesos de evaluación.

El presente Trabajo de Titulación tiene como objetivos realizar un estudio comparativo de las diferentes técnicas biométricas, implementar el sistema huella dactilar en la plataforma virtual de aprendizaje (Moodle) garantizando el control de los usuarios dentro de los procesos de evaluación, además de brindar técnicas de protección de datos que permitan la protección de los mismos.

Es así que el presente Trabajo de Titulación se divide en diferentes secciones como revisión literaria, resultados de la Investigación realizada, discusión de los resultados obtenidos, para finalizar con las conclusiones y recomendaciones del mismo.

d. Revisión de Literatura

Para estructurar esta investigación, se acudió a la revisión documental/bibliográfica, además de revisar casos de éxito relacionados con el presente Trabajo de Titulación a continuación se detalla el esquema literario dividido en capítulos.

Capítulo I

1. Plataforma Virtual De Aprendizaje: Moodle

1.1. ¿Qué es Moodle?

Moodle se ha convertido en una de las herramientas más utilizadas en la educación a distancia para la creación de cursos en línea, ya que cuenta con las características válidas para el desarrollo proporcionando un punto central de información, discusión y colaboración entre los usuarios. Moodle es una herramienta de código abierto que se encuentra bajo la Licencia Pública General GNU (GNU General Public License); quiere decir que "cualquier persona puede adaptar, extender o modificar Moodle, tanto para proyectos comerciales como no-comerciales, sin pago de cuotas por licenciamiento, y beneficiarse del costo/beneficio y flexibilidad" [1].

Esta plataforma virtual de aprendizaje (Moodle) permite tanto a los estudiantes como docentes gestionar cursos en línea personalizados, convirtiéndose en una de las herramientas más robustas, fiables utilizables por la comunidad educativa como la unidad investigadora.

1.2. Características de Moodle

A continuación se detallan de forma resumida las principales características que presenta Moodle [2].

- **Interoperabilidad**: Moodle usa el lenguaje web PHP y MySQL como base de datos, de esta manera se puede ejecutar en los diversos entornos tales como Windows, Linux, Mac, etc.
- **Escalable**: Moodle es una herramienta que puede adaptarse a las necesidades de una organización utilizando la arquitectura web que presenta la misma.

- **Personalizable**. Moodle cuenta con un panel de configuración que permite personalizarlo de acuerdo a las necesidades específicas de cada institución o empresa.
- **Económico**: Al tratarse de una herramienta libre Moodle no implica el pago de licencias u otro mecanismo de pago.
- **Seguro**. Moodle puede ser desplegado fácilmente en un servidor, o en una nube segura privada para un completo control.
- **Permite la Gestión de Perfiles de Usuario**. Permite almacenar datos de alumnos y docentes de manera que se permita establecer estadísticas socioeconómicas, fisiológicas o demográficas.
- **Permite la presentación de cualquier contenido digital**. Permite la publicación de contenidos multimedia de manera que puedan ser utilizadas como material didáctico.
- **Permite la gestión de tareas**. Los docentes pueden asignar tareas o trabajo prácticos, gestionar el horario y fecha de recepción; los alumnos pueden verificar en línea sus notas.
- **Permite realizar evaluaciones en línea**: Moodle permite publicar una lista de preguntas con alternativas o simples, permitiendo obtener las notas de manera inmediata ya que el sistema se encarga de calificar los exámenes.

En base a las características funcionales de Moodle antes mencionadas, se concluye que estas son válidas para el desarrollo de componentes que permiten una interacción entre docentes y alumnos en el ámbito educativo.

1.3. Módulos de Moodle

Moodle cuenta con una variedad de módulos como son: Módulo de tareas, Módulo de consultas, Módulo foro, Módulo diario, Módulo recurso, Módulo de encuestas, Módulo wiki, Módulo cuestionario.

1.3.1. Módulo cuestionario

Para el presente Trabajo de Titulación de utilizó el módulo cuestionario, que brinda la posibilidad al docente de crear sus evaluaciones, y así plantearlas a los usuarios del curso, estas evaluaciones pueden contener preguntas ya sea de opción múltiple, respuestas cortas, o con opciones de verdadero y falso, inclusive preguntas tipo ensayo. Las preguntas pueden ser agrupadas en una base de datos dependiendo su

categoría, a la vez estas pueden ser reutilizadas ya sea en el mismo curso o en otro curso. Además, de configurar el número de intentos, que podrá realizar el alumno, con la posibilidad de calificar y marcar cada intento; y otras múltiples facilidades y ventajas que no se tratarán en el presente Trabajo de Titulación ya que no es objeto del mismo.

Un cuestionario cuenta con las siguientes características generales, las cuales se detallarán a continuación [3]:

- **Temporalización**: Establece el límite tanto para la realización y envío del cuestionario.
- **Calificación**: Establece el número de intentos permitidos, además de la modalidad de calificación.
- **Esquema**: Delimita la forma de presentación de las preguntas, es decir el orden que van a tener las preguntas.
- **Comportamiento de las preguntas**: Establece que las preguntas con varias opciones se presentan ordenadas al azar, además de mostrar una retroalimentación al usuario.
- **Revisiones**: Se especifica qué información pueden ver los usuarios en el momento de realizar el examen.
- **Restricciones extra sobre los intentos**: Se establece una contraseña para los intentos, además del tiempo de demora entre los diferentes intentos que se le permite realizar al usuario.
- **Retroalimentación global**: Establece la posibilidad de ofrecer una retroalimentación al usuario.

Capítulo II

2. Sistemas Biométricos

2.1. Introducción

En el mundo digital actual, la autenticación personal se ha tornado en una de las actividades importantes en la interfaz computacional y humana. Es así que uno de los métodos de autenticación, se ha convertido en la herramienta más eficaz para la identificación de personas, usando características únicas ya sean fisiológicas o de

comportamiento de cada individuo lo que permite reconocer e identificar ya sea su huella dactilar, su voz, su firma etc., para distinguirlo del resto de individuos.

La implementación de sistemas biométricos ha permitido automatizar los procesos de reconocimiento de identidad, de manera que pueden ser aplicados a mejorar los procesos de seguridad, siendo así la biometría se ha convertido en un elemento clave en cuanto a técnicas de identificación.

2.2. Definición de un Sistema Biométrico.

Un Sistema Biométrico, es un sistema de reconocimiento que permite que una persona sea reconocida mediante la autenticidad de características fisiológicas y/o de comportamiento que posee. Dependiendo del contexto de la aplicación o del empleo, un sistema biométrico puede tener dos modos de operación, como sistema de verificación o de identificación [4], [5], [6] .

- Un Sistema de **Verificación** permite autenticar la identidad de la persona comparando la característica biométrica capturada, con su propio patrón (o patrones) previamente almacenados en el sistema. De manera que se pueda determinar si el usuario es quien dice ser [7].
- Un Sistema de **Identificación** reconoce a una persona a través de la búsqueda en la base de datos de patrones de una coincidencia con el patrón capturado. Siendo así permite determinar la identidad el usuario [7].

En base a estos modos de operación se determina que el presente Trabajo de Titulación, será un sistema de verificación, ya que al momento del registro permitirá almacenar en una base de datos la huella dactilar del usuario, para posteriormente realizar una comparación de la huella de entrada con la huella almacenada, es decir 1:1, y de esta manera determinar la verdadera identidad del usuario.

2.3. Sistema biométrico e identificación personal.

En un sistema tradicional de identificación personal la autenticación a una determinada entidad relacionada con la persona se efectúa a través de la contraseña y nombre de usuario. Por lo tanto los métodos tradicionales de autenticidad presentan el inconveniente de que no se puede determinar de manera fiable entre los individuos legítimos y los individuos impostores. En cambio, los métodos basados en la autenticación de la identidad a través de rasgos biométricos de una persona proporcionan una mayor fiabilidad en la identificación, ya que no pueden ser

compartidos entre las personas y a la vez garantizan que la autenticación no sea suplantada [8].

Las diferentes técnicas biométricas suelen ser clasificadas en función del rasgo humano, como pueden ser fisiológicos o de comportamiento. Dentro de las primeras se encuentran el reconocimiento de huella dactilar, de iris, de retina, de rostro entre otros. Y en las de comportamiento están el reconocimiento de voz, de firma, de la manera de andas, entre otras.

Las tecnologías biométricas más extendidas son las de reconocimiento de huella dactilar y de iris, una de las razones de esto es que fueron de las primeras en ser concebida, permitiendo así un mayor desarrollo y evolución y una reducción de costes de implementación. Por otro lado ambas técnicas son métodos muy pocos intrusivos para los usuarios finales [9].

2.4. Propiedades de los Rasgos Biométricos

Es importante identificar las propiedades que tiene los rasgos biométricos ya que de esta manera se determinar el grado de cumplimiento de cada una de ellas y así poder determinar una comparación entre los diferentes sistemas de reconocimiento biométrico.

Las propiedades de los rasgos biométricos son [7], [10], [11]:

- **Universalidad:** el rasgo biométrico existe para todos los individuos.
- **Unicidad:** el rasgo identifica unívocamente a cada individuo.
- **Permanencia:** el rasgo se mantiene invariable con el tiempo a corto plazo.
- **Inmutabilidad:** el rasgo se mantiene invariable con el tiempo a largo plazo o durante toda la vida.
- **Rendimiento:** el rasgo permite el reconocimiento de un individuo con rapidez, robustez y precisión.
- **Aceptabilidad:** el rasgo presenta la calidad de ser aceptado por la mayoría de la población.
- **Invulnerabilidad:** el rasgo permite una robustez del sistema frente a los métodos de acceso fraudulentos.

2.5. Comparación de Sistemas Biométricos.

En la actualidad existen entre 20 y 30 tecnologías biométricas implementables [12], cada una de ellas con ventajas y desventajas, donde estas tecnologías pueden convertirse en adecuadas de acuerdo a la aplicación o uso que se le quiera dar.

A continuación se realiza una comparación de los diferentes sistemas biométricos tantos fisiológicos (Huella Dactilar, Identificación Facial, Identificación por Iris, Geometría de la mano), como de comportamiento (la Voz) [6], [13], [14], [15].

2.5.1. Huella Dactilar

VENTAJAS:

- **Alta usabilidad**.- La ausencia de algún dedo en una de las manos es poco frecuente.
- **Alta permanencia.**- Estudios realizados han demostrado que la huella digital de un individuo no cambia con el pasar de los años.
- **Alta unicidad.-** Hasta la actualidad no se ha podido encontrar coincidencias de huellas digitales en personas diferentes.
- **Buenas prestaciones.-** Existen algoritmos eficientes como la comparación de huellas (minucias ocupan poco espacio para el almacenamiento).
- **Alta aceptabilidad.-** Las personas se encuentran más identificadas a utilizar su huella digital en el aseguramiento de la información.

DESVENTAJAS:

- **Media facilidad de medida.-** Los lectores electrónicos tiene costos cómodos y son fáciles de instalar y mantener, sin embargo obtener una buena imagen de la huella dactilar se ve sujeta a la presencia de suciedad, cicatrices, heridas, así mismo no se puede identificar las características específicas de la misma debido a la mala ubicación del dedo en el lector dactilar.

2.5.2. Identificación por la Voz

VENTAJAS:

- **Alta facilidad de medida.-** Coste mínimo de los equipos de hardware necesarios.
- **Alta universalidad.-** Individuos con dificultad del habla son relativamente reducidos.

- **Buenas prestaciones.-** La verificación es posible con recursos de computo muy bajos y su volumen de información almacenada es aceptable en los medios de almacenamiento actuales.
- **Alta aceptabilidad.-** Casi ningún usuario muestra resistencia, para pronunciar una frase o palabra que le permita acceder a un servicio.

DESVENTAJAS:

- **Baja permanencia.-** Los parámetros de la voz puede alterarse fácilmente por varios factores como enfermedad de gripe entre otros.
- **Baja unicidad.-** Pueden aparecer ciertos parecidos de las cuerdas vocales en ciertas personas.
- **Baja resistencia al engaño.-** Una grabación con la palabra clave puede ser considerada engañar al sistema y para suplantar identidad.

2.5.3. Identificación Facial

VENTAJAS:

- **Alta facilidad de medida.-** El coste de cámaras es bajo, siendo así su adquisición fácil.
- **Alta usabilidad.-** Cualquier rostro que no esté oculto puede ser válido para su verificación.
- **Buenas Prestaciones.-** Para la verificación se utiliza recursos de cómputo razonables, ya que el almacenamiento se da en espacios pequeños.
- **Alta aceptabilidad.-** Los usuarios aceptan este método, ya que no se convierte en limitante para el flujo de acceso.

DESVENTAJAS:

- **Baja Permanencia.-** La apariencia del rostro puede cambiar, debido a la presencia de barba, o el uso de gafas.
- **Baja Unicidad.-** Pueden existir rostros con características similares.
- **Baja Resistencia al engaño.-** El uso de máscaras, y fotografías se convierten en una manera de fraude, para confundir al sistema; sin embargo la tecnología 3D permite minimizar estos riesgos.

2.5.4. Identificación por Iris

VENTAJAS:

- **Alta usabilidad.-** Cualquier iris puede ser identificado para su debida verificación.
- **Alta Prestaciones:** Existen diferentes algoritmos de comparación, además de recursos hardware para el proceso de verificación.
- **Alta unicidad.-**Hasta la actualidad no se ha podido encontrar coincidencias de poseer el mismo iris en personas diferentes.
- **Media Permanencia.-** El iris puede cambiar por diferentes razones, como el uso de lentillas, así mismo según estudios realizados se ha determinado que el iris también envejece [16].

DESVENTAJAS:

- **Baja facilidad de medida.-** El coste de hardware es alto, siendo así su adquisición muy costosa.
- **Baja Aceptabilidad.**- Debido a que son muy robustos y difíciles de entender.

2.5.5. Geometría de la Mano

VENTAJAS:

- **Alta aceptabilidad.-** Este dispositivo es utilizado por diferentes personas como medida de verificación de acceso.
- **Alta facilidad de medida.-** El coste de este dispositivo es medio, siendo así su adquisición factible.
- **Alta usabilidad.-** Usan una cámara óptica para capturar dos imágenes ortogonales bidimensionales de la palma y lados de la mano, ofreciendo un equilibrio de fiabilidad y facilidad de su uso.

DESVENTAJAS:

- **Baja Prestaciones.-** Debido a que requiere de mucho espacio para el registro en una determina entidad.
- **Baja Permanencia.**- La geometría de la mano puede modificarse con el tiempo, debido a condiciones médicas como la artritis.

- **Baja Unicidad.-** Debido a que el diámetro de la mano puede coincidir con el de otro usuario.

2.6. Componentes de un Sistema Biométrico

Los componentes básicos de un sistema biométrico son sensores, Base de Datos, y los algoritmos.

- **Sensor.-** Es el dispositivo que captura las muestras dactilares al momento de colocar el dedo sobre la superficie del sensor de manera que estas puedan ser digitalizadas y convertidas en una plantilla biométrica [7].

Para el desarrollo del presente Trabajo de Titulación se utilizó el sensor Hamster PRO 20**,** siendo un sensor de tipo óptico. Para capturar las imágenes de las huellas dactilares, los sensores ópticos usan un prisma, una fuente de luz led y un sensor de luz [7].

El funcionamiento de los sensores ópticos se basa en extracción de puntos de la imagen que genera la huella estos puntos se denominan minucias. Al momento de colocar el dedo en la parte superior del prisma del dispositivo, las crestas entran en contacto con la superficie del mismo, mientras los valles se mantienen a cierta distancia. El lado izquierdo del prisma es iluminado mediante la luz led, esta es reflejada en los valles y aleatoriamente absorbida por las crestas [9].

Al no reflejarse la huella con el prisma, permite que las crestas no sean visibles a la imagen (siendo las líneas en blanco), mientras que las líneas claras que salen del lado derecho del prisma son enfocadas a través del sensor de modo que registra la imagen [9].

- **Bases de Datos.-** Consiste en el repositorio donde se almacenaran las plantillas biométricas inscritas, para la comparación futura. La base de datos que se ha utilizado es MySQL.

- **Algoritmos.-** Son los algoritmos usados para la extracción de características de la huella dactilar, para obtener una plantilla que será la que se va a comparar con la huella de entrada. Estos algoritmos incluyen tres funciones básicas que son: registro, verificación, e identificación.

2.7. Sistemas biométricos de huella dactilar

De acuerdo a las propiedades de los sistemas biométricos, no hay sistema alguno que cumpla con todos las características antes mencionadas, es por eso que la elección de uno de ellos se hará dependiendo el tipo de aplicación.

Los sistemas biométricos de huella dactilar son los más usados, ya que además de ser un sistema efectivo, es cómodo de aplicar y la autenticación se puede obtener rápidamente. Además de garantizar que la identidad es propia de cada persona, convirtiéndose de esta manera en un sistema muy eficiente en el ámbito de autenticación personal [12].

Motivo por el cual para el desarrollo del presenta Trabajo de Titulación se usó esta tecnología para minimizar la suplantación de identidad a la plataforma virtual de aprendizaje Moodle.

2.8. Características de las huellas dactilares

Las huellas dactilares están formadas de la siguiente manera [6]:

- ✓ **Crestas:** son segmentos de curva.
- ✓ **Valles:** son las regiones entre dos crestas adyacentes.

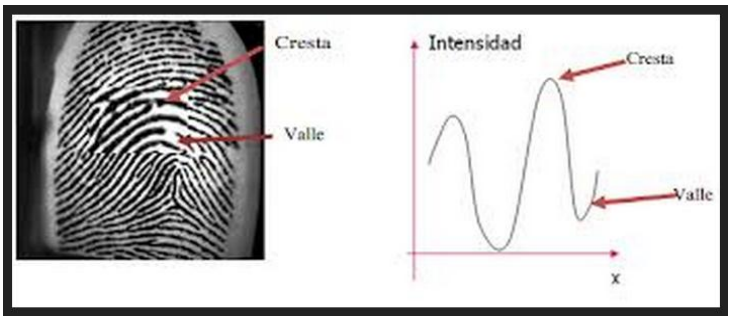


Figura 1. Crestas y Valles [6].

La huella dactilar cuenta con características únicas en las que están definidas por las minucias que son pequeñas discontinuidades formadas por el cruce y terminación de las crestas de la huella dactilar [17].

2.8.1. Tipos de Minucias

Una huella dactilar cuenta con más de 50 minucias, adecuado para el alto nivel de procesamiento necesario para evaluar todas las minucias, por lo tanto se han

clasificado teniendo en cuenta las minucias (ver Figura 2) con características únicas para la identificación de la persona [17].

Figura 2. Tipos de Minucias de una huella Dactilar [6].

2.9. Técnicas para el reconocimiento de la huella dactilar

Para el reconocimiento de la huella dactilar se la puede determinar mediante tres técnicas entre las cuales tenemos:

- **Basados en crestas:** Permite analizar cada una de las huellas mediante las crestas, que son los segmentos de curva de la huella que la componen (ver Figura 3), cuya captura se basa en puntos específicos de las curvas que componen una cresta.

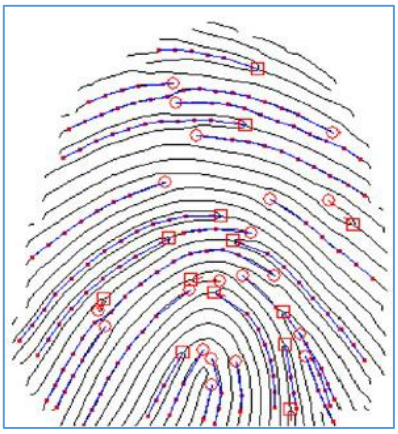


Figura 3. Captura de Huella Basa en Crestas [18].

- **Basados en texturas:** Permite el análisis de la huella mediante patrones de crestas y valles cuya textura está orientada con frecuencia espacial y orientación localmente constante.

- **Frecuencia=** variación periódica entre crestas y valles.
- **Orientación =** dirección del flujo de crestas.

Funcionamiento de captura de la huella dactilar por textura (ver Figura 4).

Figura 4. Captura de Huella Basa en Texturas [18].

- **Basados en Minucias:** Permite la captura de la huella dactilar mediante características específicas de minucias, que son características únicas para la identificación de la persona, además está captura se basa en el trio de minucias al formar tres puntos específicos de características que componen la huella facilitando su captura (ver Figura 5).

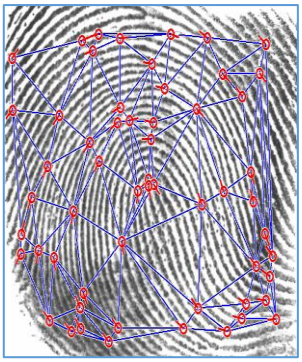


Figura 5. Captura de Huella Basa en Minucias [18].

2.10. Proceso de Registro en el Sistema.

Para el acceso a la plataforma virtual de aprendizaje Moodle, el usuario tendrá que registrar su identidad en el sistema, esto se efectúa obteniendo o capturando los parámetros biométricos, dentro del registro se diferencias tres fases distintas que son Captura, Procesamiento e Inscripción.

2.10.1. Captura:

En esta fase se hace uso del sensor biométrico para extraer los parámetros biométricos de la huella dactilar que son las minucias.

2.10.2. Procesamiento:

Se genera una plantilla o patrón de huellas con las características capturadas de la huella como son ubicación, dirección del final de las minucias.

2.10.3. Inscripción:

La plantilla procesada se guarda en un medio de almacenamiento adecuado. Una vez que la inscripción está completa, el sistema puede autenticara las personas mediante el uso de esta plantilla, (ver Figura 6).

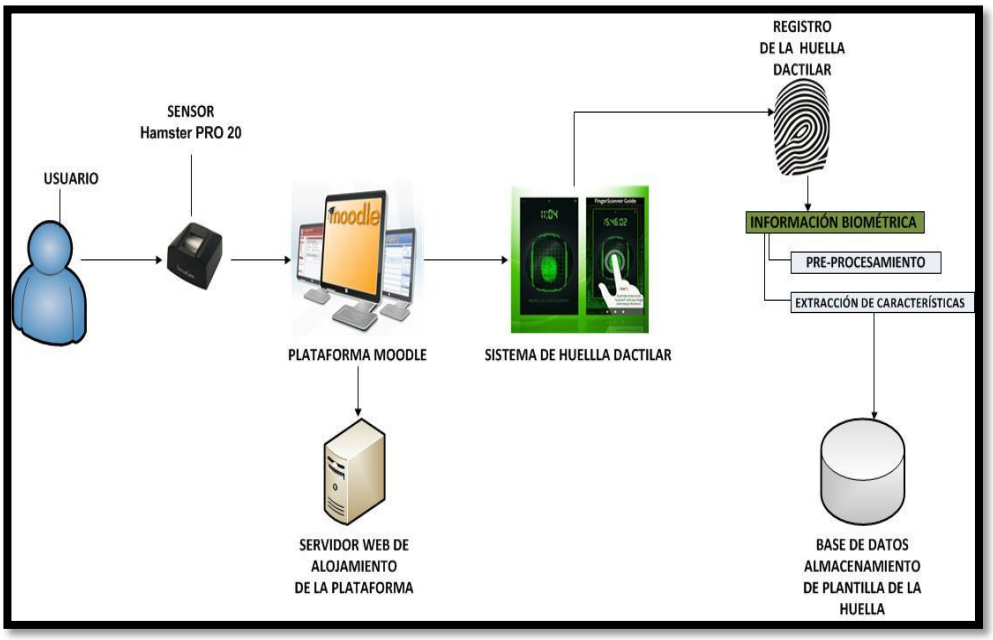


Figura 6. Proceso de Inscripción.

2.10.4. Verificación.

En el proceso de la verificación, el usuario primeramente tendrá que identificarse mediante un nombre, e ingresar su huella dactilar para de este modo el sistema recoge estos dos parámetros, para buscar el nombre del usuario en la base de datos y verificar que este exista y en caso de encontrarlo verificar el siguiente parámetro que es la huella dactilar, comparándola con la ya almacenada, dando como como resultado un aceptado o rechazado [19], (ver Figura 7).

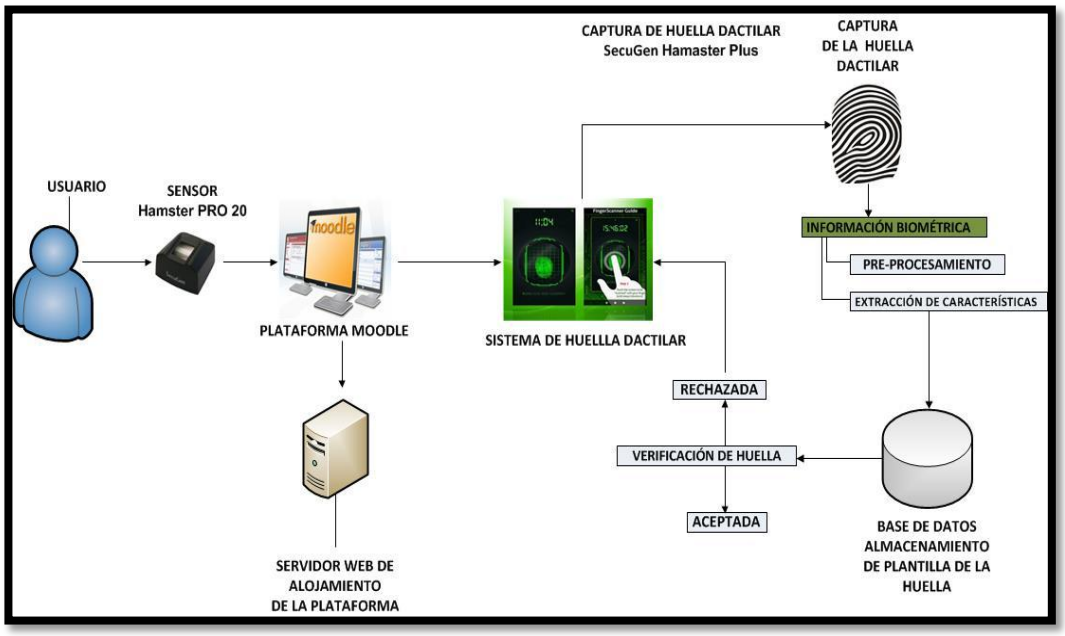


Figura 7. Modo Verificación.

Capítulo III

3. Análisis de la situación actual.

Dada la importancia que tiene la evaluación en el proceso de enseñanza aprendizaje, dentro de cualquier modalidad, esta forma parte crucial del diseño pedagógico en cada una de las actividades de formación en la educación, razón por la cual es necesario que estas evaluaciones presente fiabilidad; y más aún si hablamos de las evaluaciones en línea [20].

Una de las desventajas que presenta Moodle es la suplantación de identidad, de ahí que muchos docentes manifiestan su preocupación de que se produzca este riesgo, y no sea el propio estudiante quien genere los contenidos ya que, en realidad, no se sabe quién realmente está detrás de cada respuesta de la evaluación.

Es por eso la necesidad de buscar métodos que permitan eliminar o evitar la suplantación de identidad en los procesos de evaluación que se realizan en la plataforma de Moodle.

Es así que el presente Trabajo de Titulación aplica la biometría como una técnica diseñada para minimizar la suplantación de identidad, de tal manera que identifique y verifique la identidad de los usuarios que ingresan la plataforma. El concepto de

biometría aplicado a la evaluación a distancia parte de la idea que los procesos de evaluación sean auténticos y proporcione credibilidad a la calidad de los cursos impartidos en las plataformas virtuales de aprendizaje [21].

3.1 Casos de éxito.

En el desarrollo del presente Trabajo de Titulación se ha seleccionado un caso de éxito específico, donde se ha implementado una medida de seguridad biométrica a una plataforma virtual de aprendizaje [21]. Así mismo se detallan casos de éxito donde la implementación de la huella dactilar ha sido el complemento a la seguridad a una aplicación específica.

- Sistema de Verificación por Huella Dactilar en Exámenes en Moodle
- Análisis de la Implementación de Lectores de Huella Dactilar y Firmas Digitales en los Registros de un Software de Historia Clínica Electrónica en Colombia.
- Sistema de Autenticación Biométrica de Huella Dactilar asistido por Interfaz de Voz para el Control de Accesos.

A continuación se analiza los casos de éxito describiendo el proyecto.

3.1.1 Sistema de Verificación por Huella Dactilar en Exámenes en Moodle.

3.1.1.1 Descripción del Proyecto.

El proyecto denominado "Sistema de Verificación por Huella Dactilar en Exámenes en Moodle", permite brindar un grado más de seguridad a la mencionada Plataforma Virtual, proyecto liderado por Rosario Gil, Ingeniera en Telecomunicaciones, quien lo implemento en la Universidad Nacional de Educación a Distancia.

Mediante un análisis a las vulnerabilidades en cuanto a seguridad en Moodle se comprueba que los sistemas de acceso no aseguran la identidad de las personas que acceden, en general, a aquellos recursos protegidos y solo accesibles a un público en concreto pueden seguir política de asignación de roles o gestión de accesos por parte de un administrador. Además, muchas páginas disponen de herramientas de auditoría por defecto, que si bien la privacidad de los usuarios se verá reducida, pueden monitorizar y trazar el rastro de acciones no permitidas [22].

En base a esto se pretende busca un medio para autenticar a los usuarios y asegurar la identidad del mismo. La investigación que se buscó en este artículo, tuvo como

objetivo combinar las formas tradicionales de identificación con la autenticación para determinar que el usuario es quien dice ser [23].

La experiencia se realizó en comunidades educativas dentro del ámbito de la universidad especialmente en los estudios impartidos a distancia donde se llega a más personas con mayor facilidad y mayor calidad de recursos que en el pasado, permitiendo que se puedan impartir cursos desde cualquier localización en el mundo, donde no se tiene un control a los estudiantes en relación con el centro de enseñanza [24].

Tomando en cuenta el método de enseñanza a distancia impartido por cada uno de los docentes, este caso de éxito permitido minimizar la suplantación de identidad mediante la autenticación por huella dactilar aplicada a una plataforma virtual de aprendizaje como es Moodle, mejorando la calidad de estudio y fiabilidad en los cursos seguidos a distancia.

3.1.2 Análisis de la Implementación de Lectores de Huella Dactilar y Firmas Digitales en los Registros de un Software de Historia Clínica Electrónica en Colombia.

3.1.2.1 Descripción del Proyecto.

Este proyecto se enfoca en la seguridad e integridad de los datos de un Sistema de Historia Clínica Electrónica, razón por la cual se propone la implementación de lectores de Huella Dactilar como un complemento a la seguridad y acceso de la información médica de dicho Sistema.

Antes de elegir la herramienta electrónica que complementara el Sistema, se debe de tomar en cuenta: Quién, Cuándo y Porqué debe o puede acceder un usuario a cierta información médica.

Es importante mencionar que el Sistema de Historia Clínica Electrónica usa el modelo de seguridad tradicional como es USUARIO + CLAVE, modelo que no garantiza la confidencialidad e integridad de la información médica [25], generando así: la modificación o perdida de la información médica del paciente almacenada en el sistema y el acceso no autorizado a la información médica del paciente violando el secreto médico [25].

Luego de un análisis para eliminar o minimizar los riesgos antes mencionados, se determinó la implementación de lectores de huella dactilar y el uso de firmas digitales,

asegurando así la integridad de la información. Para la implementación se solicita el SDK al fabricante del dispositivo para poder crear la aplicación de huella dactilar que fue integrada totalmente a la Historia Clínica Electrónica.

Finalmente esta implementación permite eliminar casi en su totalidad los riesgos detectados en el acceso y manejo de la información, aumentando así la confianza de los pacientes en que sus datos están mucho más seguros [25].

3.1.3 Sistema de Autenticación Biométrica de Huella Dactilar asistido por Interfaz de Voz para el Control de Accesos.

3.1.3.1 Descripción del Proyecto.

Este proyecto presenta el desarrollo de un sistema electrónico digital para el control de accesos usando la huella dactilar ya que es mucho más difícil de duplicar, facilitando el acceso a los usuarios.

Además de contar con la huella dactilar, también está compuesta por una interfaz de voz, permitiendo facilitar el acceso a inmuebles de los usuarios, en lugar de usar llaves. Siendo así el usuario podrá desplazar su dedo por el dispositivo para poder abrir la puerta; de este modo permite garantizar la seguridad en el acceso a sus inmuebles, además el dispositivo funciona de forma autónoma sin depender de un sistema externo para realizar dicha operación [7].

a. Materiales y Métodos

1. Métodos

Entre los métodos que se utilizó dentro del presente Trabajo de Titulación está el Científico el cual sirve para organizar y sistematizar el proceso investigativo del presente trabajo para la demostración de resultados; en donde se partirá de la revisión de casos de éxito sobre sistemas de verificación de huella dactilar aplicados a los procesos de evaluación en entornos virtuales de aprendizaje (Moodle), recopilación de información hasta llegar a la obtención de resultados reflejados en las conclusiones.

Otro de los métodos que utilizamos es el método analítico, este facilita el análisis para llegar a soluciones adecuadas previa separación de cada problema en sub problemas, que contribuirá a profundizarnos en el objetivo de estudio en cuestión.

2. Técnicas

Los métodos e instrumentos que utilizamos para la recopilación de la información son los siguientes:

La técnica de la observación contribuyo en la determinación de todos los inconvenientes que se presentaron en el desarrollo de las actividades, y los problemas que se encontraron en los procesos de evaluación en la plataforma virtual de aprendizaje (Moodle), para su posterior mejora mediante la técnica de autenticación por huella dactilar.

La técnica de investigación bibliográfica, permitió sustentar la base de la teoría de la investigación, a través de fuentes bibliográficas confiables, artículos científicos, casos de éxito, fuentes informáticas.

Lectura comprensiva permitió obtener un conocimiento ordenado y sistemático de la realidad o de los acontecimientos hechos o ideas relacionadas con el tema específico.

3. Materiales

- **MySQL.-** Es un sistema de gestión de base datos relacional, multihilo y multiusuario, debido a que es utilizada en aplicaciones web, en distintas plataformas y tomando en cuenta sus características optamos por este tipo de base de datos para almacenar y mantener protegida la información que se maneje en la aplicación de verificación por huella dactilar.

- **PHP.-** (acrónimo recursivo de PHP: Hypertext Preprocessor) es un lenguaje de código abierto adecuado para el desarrollo web cuyo contenido es dinámico, que se incorpora directamente en el documento HTML. Hemos optado por utilizar PHP, ya que permite el soporte para gran cantidad de bases de datos, ofreciendo una solución simple, para paginaciones dinámicas de fácil programación con Moodle [26].

- **Apache.-** Es un servidor web HTTP de código abierto que permite acceder a páginas web alojadas en un ordenador, entre las características que presenta tenemos mensajes de error altamente configurables, bases de datos de autenticación, negocio de contenido, entre otras. Tomando en cuenta sus características hemos optado por Apache por múltiples razones como disponibilidad, multiplataforma, facilidad de instalación, pocos recursos necesarios, precio, disponibilidad del código fuente [27].

- **Moodle 2.6-** Es una Plataforma Virtual de Aprendizaje, es una herramienta de código abierto bajo la Licencia Pública General GNU que permite a los educadores, administradores y estudiantes, crear y gestionar ambientes de aprendizaje en línea personalizados, de acuerdo a estas características hemos optado escoger la plataforma virtual de aprendizaje Moodle ya que facilita su uso al tratarse de código abierto y fácil gestión, permitiendo de esta manera que se pueda integrar con el sistema de huella dactilar para el control de suplantación de identidad dentro de los procesos de evaluación contenidos en estas plataformas de enseñanza [2].

- **Lector de Huella Dactilar Biométrico SecuGen HamsterPRO 20.-** Para comparar exitosamente las imágenes de huellas dactilares es imprescindible que dichas imágenes tengan suficiente contraste y resolución (500dpi), hayan sido comprimidas correctamente con WSQ y no presenten distorsiones, razón por la cual se ha optado por utilizar el lector de huella SecuGen Hamster PRO 20.

  SecuGen Hamster PRO 20, es un escáner óptimo de huellas dactilares USB (ver Figura 8). El escáner tiene un diseño compacto con soporte extraíble, al poner el dedo sobre este dispositivo genera una imagen digital de la huella dactilar. SecuGen Hamster PRO 20cuenta con un software (SDK) el mismo que es

encargado de verificar las características propias de la huella como son las crestas y los surcos [28].

Figura 8. Lector de Huella SecuGen Hamster PRO 20.

De acuerdo a las características que proporciona este dispositivo hemos optado por este dispositivo compacto, ligero y portátil, que facilita la captura de las huellas para que se puedan almacenar en nuestra base de datos, tiene un único algoritmo de procesamiento de imágenes de huellas dactilares que extrae las minucias con mucha precisión, e incluso las difíciles de analizar ya sea: secos, húmedos, de edad o con cicatrices [28]. En el Anexo 1., se indica las especificaciones técnicas del dispositivo.

- **Driver SecuFMASetup.**

El lector de SecuGen Hamster PRO 20 es un dispositivo periférico que requiere de un controlador para activar o controlar el dispositivo, permitiendo que se detecte el dispositivo al momento que este sea conectado. Ver Anexo 3. Subsección 3.3 Instalación de driver SecuFMASetup.

- **FDx SDK Pro for Windows v3.7_J14**

  El FDXSDK_Pro_Win_v.3.54 es el kit de desarrollo de software del dispositivo biométrico Hamster PRO 20 que permite su funcionamiento sobre Windows. Controla las funciones de captura y validación de la huella dactilar [28]. Ver Anexo 3. Subsección 3.1 Instalación de FDx SDK Pro for Windows v3.7_J14.

- **FDx SDK Pro for Java v1.4 rev593**

  Un conjunto de funciones implementadas bajo el código de Java, que permiten la comunicación del dispositivo biométrico con el sistema operativo, a través de una Biblioteca de Enlace Dinámico (DLL por sus siglas en inglés), que soporta el

SDK de Hamster Plus y así poder controlar desde código Java su funcionamiento. Ver Anexo 3. Subsección 3.2 Instalación FDx SDK Pro for Java.

- **Entorno de desarrollo NetBeans.**

  NetBeans es un entorno de desarrollo integrado de código abierto, que permite que las aplicaciones sean desarrolladas a partir de un conjunto de componentes de software llamados módulos, debido a que es una plataforma que facilita el desarrollo a programadores optamos por el uso de este entorno de desarrollo agilizando la implementación del proyecto ya que cuenta con una interfaz muy amigable.

- **Lenguaje de Programación Java.**

  Java es un lenguaje de programación comercializada por primera vez en 1995 por Sun Microsystems en 1995 [29]. Java es un lenguaje orientado a objetos de propósito general, presta mucha atención a la seguridad desde el ámbito del programador, hasta el ámbito de ejecución en la máquina virtual [30].

4. Metodología

Para la implantación del presente Trabajo de Titulación se utilizó la metodología Scrum, metodología que nos permite llevar un orden de las actividades que se deben cumplir, alcanzando un esquema de desarrollo adecuado.

La metodología Scrum es uno de los métodos ágiles de proyectos de desarrollo de software, basada en un proceso de trabajo constante, iterativo e incremental. Además permite que el desarrollo de la aplicación sea muy simple, que requiera de un esfuerzo, ya que no se basa en un plan, si no según la evolución y adaptación del proyecto.

La aplicación de esta metodología (ver Figura 9) consta de diferentes etapas o tareas que se deben seguir, las cuales se describen a continuación:

La primera etapa comienza con la elaboración del llamado Product Backlog. Se trata de un archivo genérico que recoge el conjunto de tareas, los requerimientos y funcionalidades requeridas por la aplicación de la Huella Dactilar.

La segunda etapa pasa por la definición del Sprint Backlog, documento que recoge las tareas a realizar para llevar a cabo el desarrollo de la aplicación como son los casos de uso, diagramas de secuencia, y el desarrollo en sí de la aplicación.

El Sprint es el periodo en el que se realizan todas las acciones pactadas en el Sprint Backlog y supone entregas parciales que se someterán a pruebas piloto para ver si cumple los objetivos planteados.

Todas las acciones que realicemos tienen un control. Es en el Burn Down donde marcamos el estado y la evolución del proyecto indicando las tareas y requerimientos que deben ser tratados.

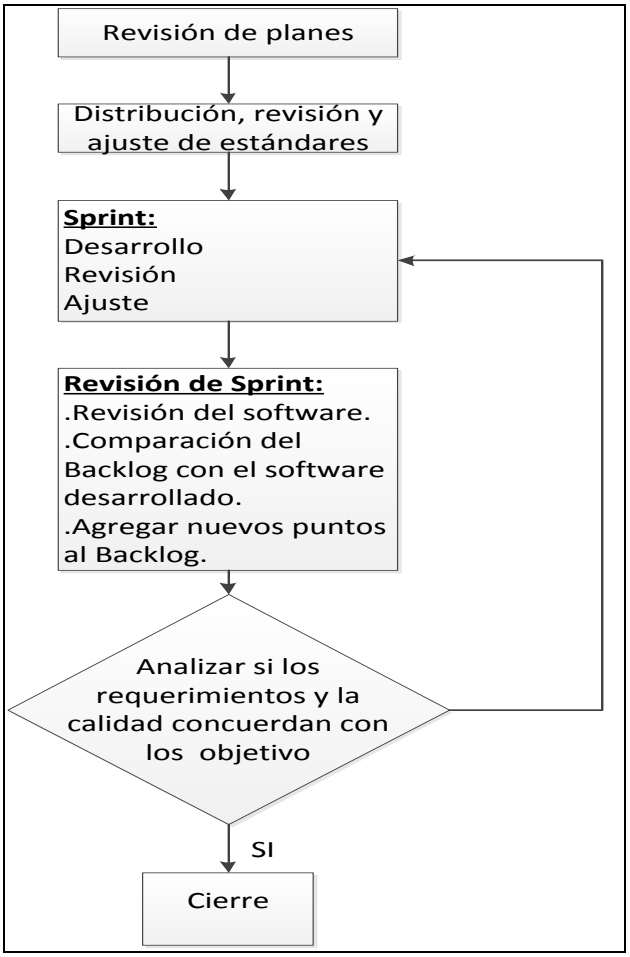


Figura 9. Etapas de la Metodología SCRUM.

b. Resultados

En este apartado se plasma el estudio y desarrollo efectuado sobre la integración del lector biométrico de huella dactilar a la plataforma virtual de aprendizaje Moodle, el mismo que se llevó a cabo de acuerdo a los objetivos planteados, estableciendo un desarrollo por cada uno de los mismos, los cuales se detallan a continuación.

Fase 1: **Comparar y seleccionar tecnologías biométricas, que se adapten dentro de una plataforma virtual de aprendizaje**.

En esta fase se efectuó la determinación que debe cumplir un sistema biométrico, a continuación se presenta un resumen comparativo de las técnicas biométricas más utilizadas atendiendo a las propiedades mencionadas en el **CAPITULO II sección 2.4 Propiedades de los rasgos biométricos**.

Así mismo se representa el grado de cumplimiento de las propiedades de diferentes técnicas biométricas establecidas en los siguientes parámetros de medición: **A:** alto; **M:** medio; **B:** bajo, estos parámetros son tomados de acuerdo a las ventajas y desventajas que poseen las técnicas biométricas durante su aplicación.

TABLA I. CUADRO COMPARATIVO DE LAS PROPIEDADES DE DIFERENTES TÉCNICAS BIOMÉTRICAS.

TÉCNICAS BIOMÉTRICAS	**Usabilidad**	**Permanencia**	**Unicidad**	**Prestaciones**	**Aceptabilidad**	**Facilidad de medida**
Huella dactilar	A	A	A	A	A	M
Identificación por la voz	A	B	B	A	A	A
Identificación Facial	A	B	B	A	A	A
Identificación Iris	A	M	A	A	B	B
Geometría de la mano	A	B	B	B	A	A

Concluyendo que los sistemas biométricos en general, y especialmente los sistemas de reconocimiento automático basado en huellas dactilares, representan una importante área de investigación y desarrollo tecnológico, ya que tienen un amplio campo de aplicación y un mercado potencial creciente de acuerdo a sus propiedades observadas en la TABLA I, siendo una de las técnicas con mayor grado de cumplimiento frente a las demás técnicas y además es una de las que mejor se acopla para llevar a cabo el presente Trabajo de Titulación.

Además para el cumplimiento de esta fase se obtuvo resultados mediante el estudio de casos de éxito, en los cuales de resume a continuación la importancia de los mismos.

"Sistema de Verificación por Huella Dactilar en Exámenes en Moodle"

En España, la Universidad Nacional de Educación a Distancia (UNED), desarrollo y puso en marcha este proyecto, teniendo gran acogida por parte de los alumnos con modalidad de estudios a distancia, y lo más importante presentando una alternativa de solución frente al riesgo de suplantación de identidad a los procesos de evaluación, para de esta manera mejorar la calidad de las evaluaciones.

"Análisis de la Implementación de Lectores de Huella Dactilar y Firmas Digitales en los Registros de un Software de Historia Clínica Electrónica en Colombia"

La Historia Clínica Electrónica almacena información médica confidencial por lo que requiere tener un método de autenticación que permita controlar el acceso de los usuarios. La implementación de lectores biométricos es una buena alternativa para minimizar estos riesgos, una vez integrado el sistema de huella dactilar al sistema de Historia Clínica Electrónica se puede identificar que se minimizan los accesos indebidos, convirtiéndose en una buena alternativa de control de acceso.

"Sistema de Autenticación Biométrica de Huella Dactilar asistido por Interfaz de Voz para el Control de Accesos"

Para el control de accesos de los usuarios a los inmuebles en lugar de usar llaves se ve la necesidad de usar la huella dactilar combinado con reconocimiento de voz, la elección de la huella dactilar se da porque es una de las "llaves" más difíciles de duplicar, porque es una característica única en cada ser humano. Basta que el usuario

pase el dedo por el lector y diga palabras claves mediante el dispositivo de voz, para que la puerta de su inmueble se abra.

Fase 2: **Integrar el sistema de autenticación a la Plataforma Virtual de Aprendizaje (Moodle).**

En esta fase se desarrolla el Sistema de Reconocimiento de Huella Dactilar utilizando Applets y la integración con la Plataforma Virtual Moodle, cuyo desarrollo se explica a continuación.

2.1 DISEÑO

2.1.1 REQUERIMIENTOS

TABLA II. REQUERIMIENTOS FUNCIONALES.

CÓDIGO	DESCRIPCIÓN	CATEGORÍA
RF001	El sistema permitirá al usuario capturar y registrar la Huella Dactilar.	Visible
RF002	El sistema permitirá al usuario almacenar su identidad con su Huella Dactilar.	Visible
RF003	El sistema permitirá al usuario verificar su identidad mediante la Huella Dactilar.	Visible
RF004	El sistema permitirá al usuario verificar su identidad mediante la Huella Dactilar dentro los procesos de evaluación.	Visible
RF005	El sistema permitirá bloquear la cuenta del usuario después de tres intentos erróneos.	Visible

TABLA III. REQUERIMIENTOS NO FUNCIONALES.

CÓDIGO	DESCRIPCIÓN	CATEGORÍA
RNF001	El sistema será desarrollado bajo la plataforma de programación Java.	Oculto
RNF002	El sistema se desenvolverá bajo entorno web utilizando para ello Applets integrados a la Plataforma Virtual de Aprendizaje Moodle.	Oculto
RNF003	El sistema será multiusuario.	Oculto
RNF004	El sistema utilizará como base de datos MySql.	Oculto

2.1.2 DIAGRAMAS DE CASOS DE USO

Los casos de uso nos permiten identificar las funciones del sistema biométrico integrado a la Plataforma Virtual Moodle.

CASO DE USO REGISTRO:

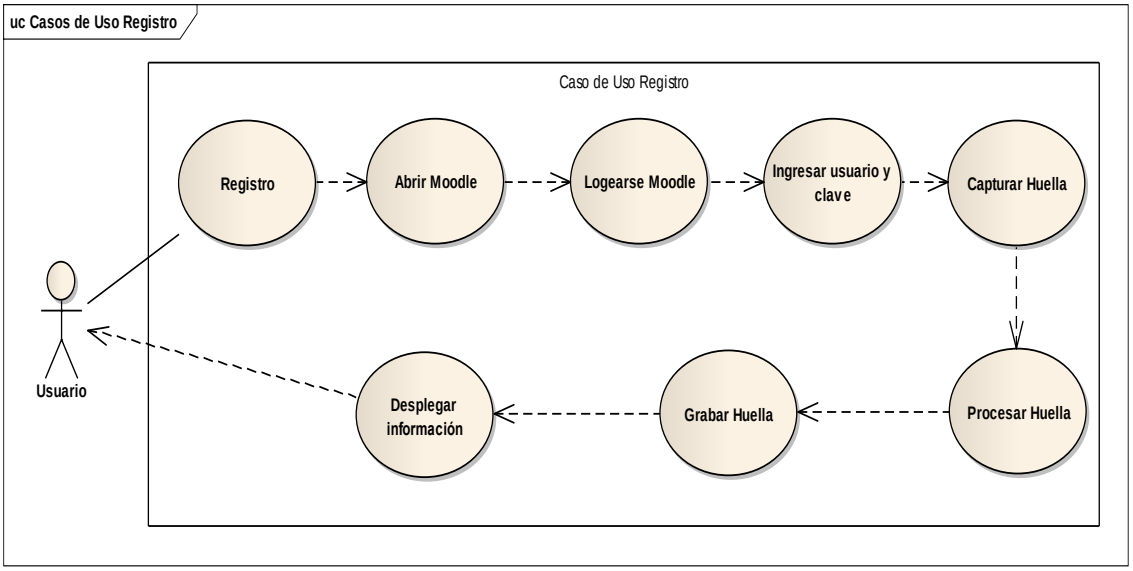


Figura 10. Diagrama del Caso de Uso Registro.

CASO DE USO VERIFICACIÓN:

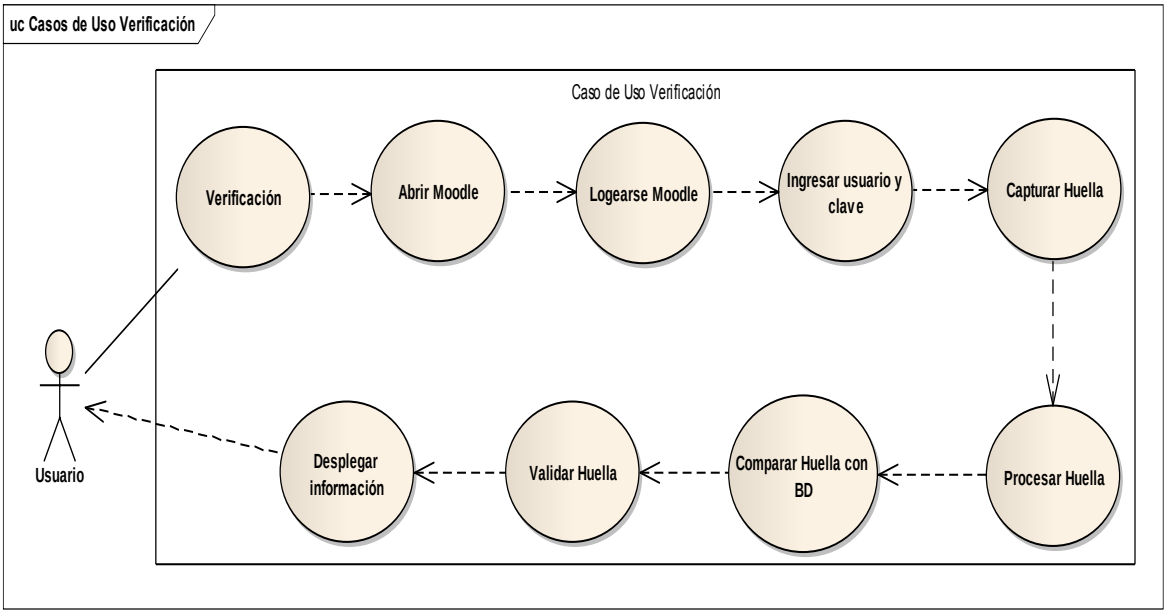


Figura 11. Diagrama del Caso de Uso Verificación.

CASO DE USO VERIFICACIÓN PROCESOS DE EVALUACIÓN:

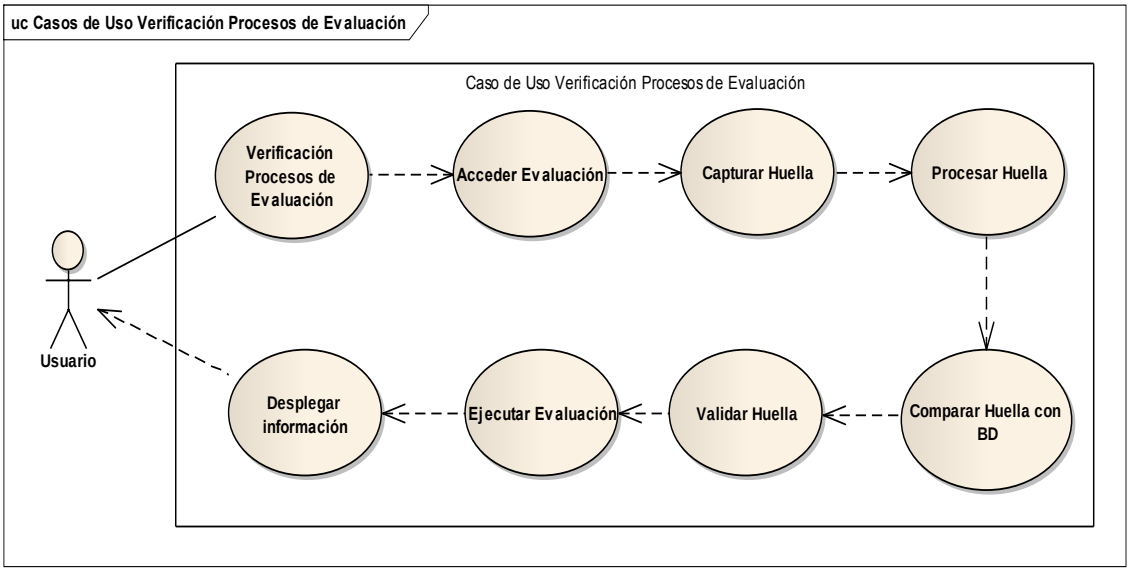


Figura 12. Diagrama del Caso de Uso Verificación Procesos de Evaluación.

2.1.3 DESCRIPCIÓN DE LOS CASOS DE USO

CASO DE USO: Registro

TABLA IV. CASO DE USO REGISTRO

Nombre:	Registro	**Código:** 003
Requerimiento Funcional:	RF001, RF002	
Actores:	Usuario, Base de Datos	
Objetivo:	Permitir al Usuario registrar su Huella Dactilar	
Descripción:	Que el usuario previamente registrado en la Plataforma Virtual Moodle pueda registrar su Huella Dactilar.	
Precondiciones:	Haber ingresado a la Plataforma Virtual Moodle	
Poscondiciones:	Huella Dactilar del usuario almacenada en la Base de Datos	
FLUJO NORMAL:	1. El usuario ingresa su nombre y contraseña. 2. El sistema verifica los datos ingresados con los de la Base de Datos. 3. El sistema presenta la pantalla de Registro de Huella Dactilar. 4. El usuario ingresa su Huella Dactilar. 5. El sistema valida que el campo de captura de Huella Dactilar no este vacío. 6. El sistema procesa la Huella Dactilar. 7. El sistema guarda la Huella Dactilar. 8. El usuario tiene acceso a la Plataforma Virtual Moodle.	
FLUJO ALTERNO:	**A. PANTALLA VERIFICACIÓN** A.3. El Sistema presenta la pantalla de Verificación de Huella Dactilar. A.4. El caso de uso continúa en el paso 4 del flujo normal de eventos. **B. CAMPOS OBLIGATORIOS VACÍOS** B.5. El sistema muestra un mensaje de campos obligatorios vacíos. B.4. El caso de uso continúa en el paso 3 del flujo normal de eventos. **C. HUELLA NO VALIDA** C.6. El sistema muestra un mensaje de error de obtención de imagen. C.7. El caso de uso continúa en el paso 4 del flujo normal de eventos.	

CASO DE USO: Verificación

TABLA V. CASO DE USO VERIFICACIÓN

Nombre:	Verificación	**Código:** 002
Requerimiento Funcional:	RF003	
Actores:	Usuario, Base de Datos	
Objetivo:	Al usuario permitir	
Descripción:	Permitir a un usuario registrado hacer	
Precondiciones:	Haber ingresado a Moodle	
Poscondiciones:	El usuario es autenticado	
FLUJO NORMAL:	1. El usuario ingresa su nombre y contraseña. 2. El sistema verifica los datos ingresados con los de la Base de Datos. 3. El sistema presenta la pantalla de Verificación de Huella Dactilar. 4. El usuario ingresa su Huella Dactilar. 5. El sistema valida que el campo de captura de Huella Dactilar no este vacío. 6. El sistema procesa la Huella Dactilar. 7. El sistema compara la Huella Dactilar con la almacenada en la base de datos. 8. El usuario tiene acceso a la Plataforma Virtual Moodle.	
FLUJO ALTERNO:	**A. PANTALLA REGISTRO** A.3. El Sistema presenta la pantalla de Registro de Huella Dactilar. A.4. El caso de uso continúa en el paso 4 del flujo normal de eventos. **B.** A.2. El Sistema bloquea la cuenta del usuario si los intentos fallidos llega a tres. **C. CAMPOS OBLIGATORIOS VACÍOS** B.5. El sistema muestra un mensaje de campos obligatorios vacíos. B.4. El caso de uso continúa en el paso 3 del flujo normal de eventos. **D. HUELLA NO VALIDA** C.6. El sistema muestra un mensaje de error de obtención de imagen. C.7. El caso de uso continúa en el paso 4 del flujo normal de eventos.	

CASO DE USO: Verificación Procesos de Evaluación

TABLA VI. VERIFICACIÓN PROCESOS DE EVALUACIÓN

Nombre:	Verificación Procesos de Evaluación	**Código:** 003
Requerimiento Funcional:	RF004	
Actores:	Usuario, Base de Datos	
Objetivo:	Al usuario permitir rendir la evaluación luego de verificar su huella dactilar	
Descripción:	Antes de rendir una evaluación es necesario que el usuario verifique su huella dactilar.	
Precondiciones:	Haberse autenticado a la Plataforma Virtual Moodle	
Poscondiciones:	Realizar la Evaluación	
FLUJO NORMAL:	1. El usuario hace clic en el botón **Comenzar Evaluación.** 2. El Sistema muestra la pantalla de Verificación. 3. El usuario ingresa su huella dactilar. 4. El sistema valida la huella dactilar 5. El sistema valida que el campo de captura de Huella Dactilar no este vacío. 6. El sistema procesa la Huella Dactilar. 7. El sistema compara la Huella Dactilar con la almacenada en la base de datos. 8. El usuario puede rendir la evaluación.	
FLUJO ALTERNO:	**A. CAMPOS OBLIGATORIOS VACÍOS** B.5. El sistema muestra un mensaje de campos obligatorios vacíos. B.4. El caso de uso continúa en el paso 3 del flujo normal de eventos. **B. HUELLA NO VALIDA** C.6. El sistema muestra un mensaje de error de obtención de imagen. C.7. El caso de uso continúa en el paso 4 del flujo normal de eventos.	

2.1.4 DIAGRAMAS DE SECUENCIA

Los siguientes diagramas de secuencia muestran los sucesos entre el usuario y el sistema.

DIAGRAMA DE SECUENCIA 001: Registro (DS001).

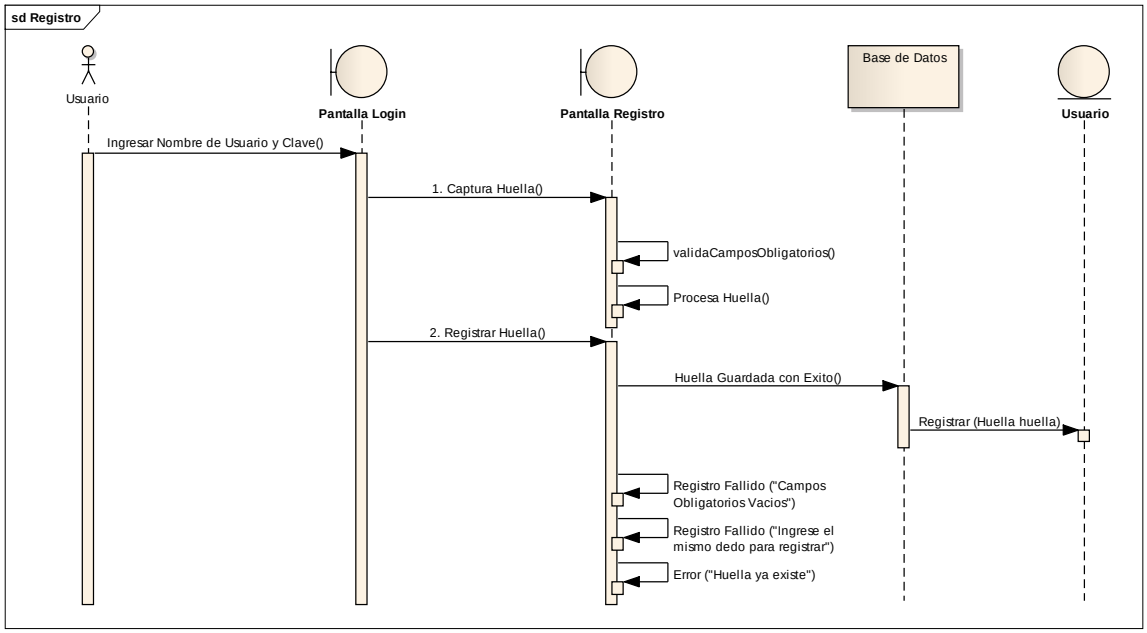


Figura 13. Diagrama de Secuencia: Registro.

DIAGRAMA DE SECUENCIA 002: Verificación (DS002).

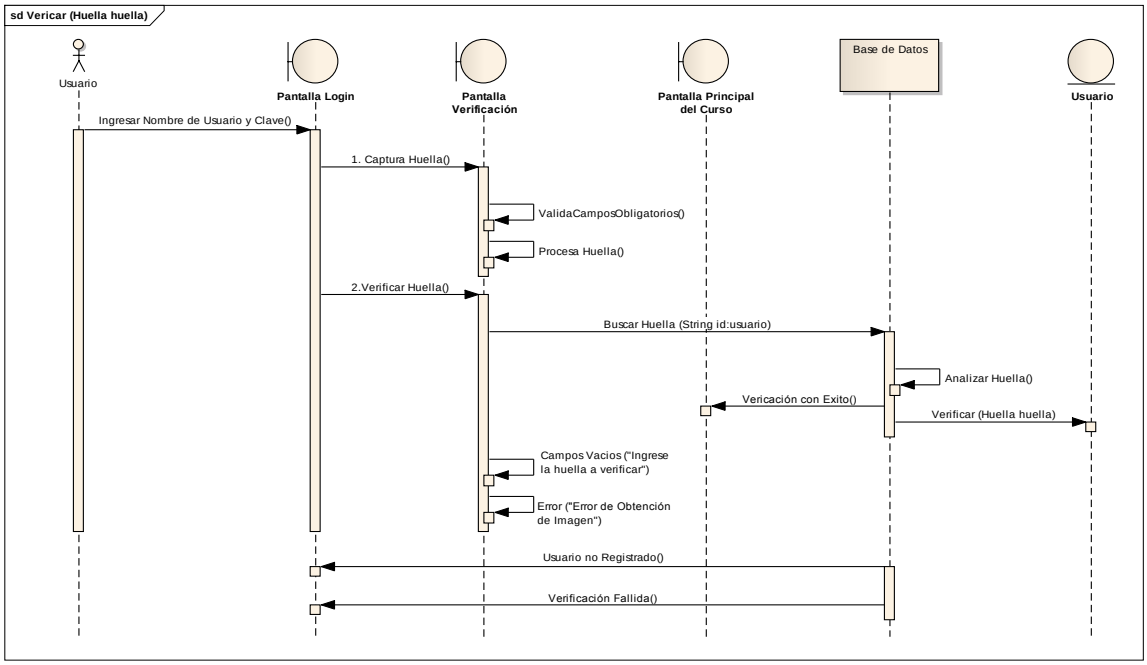


Figura 14. Diagrama de Secuencia: Verificación.

DIAGRAMA DE SECUENCIA 003: Verificación en los Procesos de Evaluación (DS003).

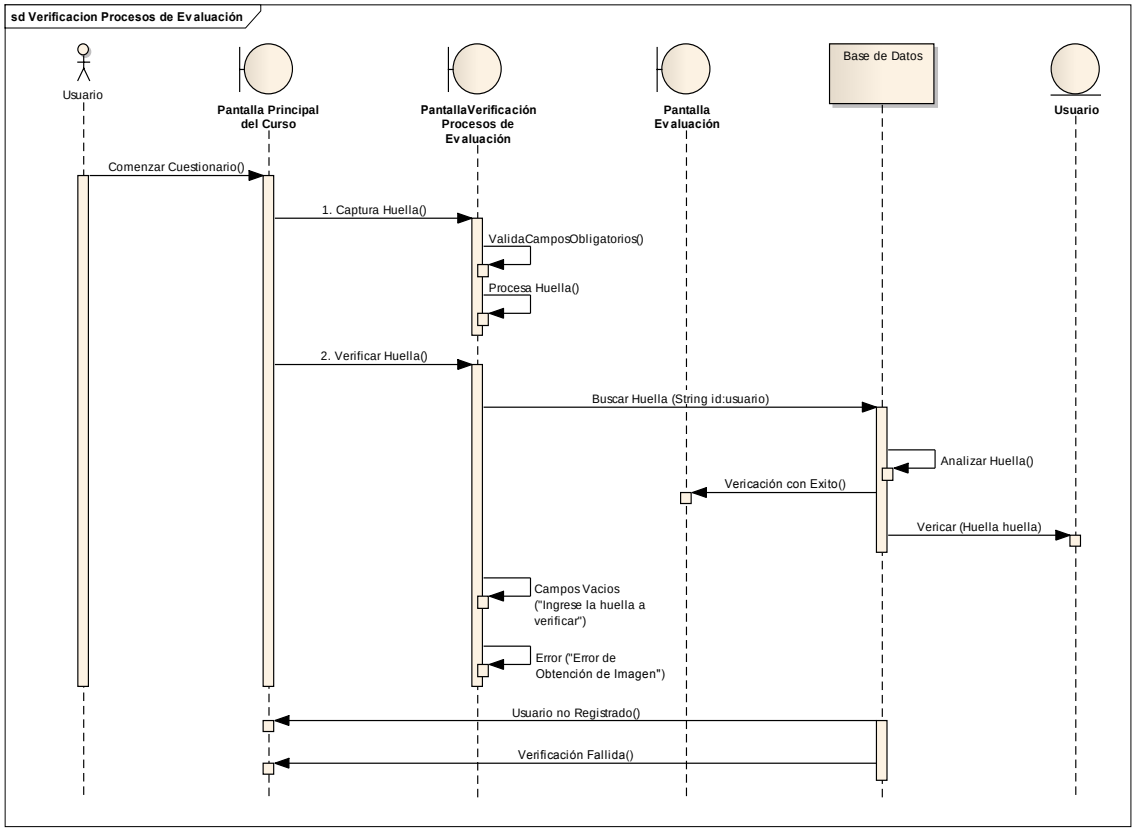


Figura 15. Diagrama de Secuencia: Verificación en los Procesos de Evaluación.

2.2 Desarrollo del Prototipo

El sistema que permite el registro de la Huella Dactilar está desarrollado en el lenguaje de programación Java utilizando Applets y NetBeans como entorno de desarrollo principal, y como gestor de base de datos se ha utilizado MySql, que a la vez es utilizada por la Plataforma Moodle.

Para el proceso de registro se creó el Applet llamado “Registro Huella”, encargada de la captura y análisis de la huella para su almacenamiento en la base de datos.

Para el proceso de verificación se creó el Applet llamado “Verificación Huella”, que realiza una comparación de las características de la huella ingresada y la huella almacenada.

Los paquetes utilizados para extraer la huella dactilar desde NetBeans son los siguientes paquetes:

TABLA VII. LIBRERÍAS DEL DISPOSITIVO SECUGEN HAMSTER PRO 20.

```
import SecuGen.FDxSDKPro.jni.JSGFPLib;
import SecuGen.FDxSDKPro.jni.SGDeviceInfoParam;
import SecuGen.FDxSDKPro.jni.SGFDxDeviceName;
import SecuGen.FDxSDKPro.jni.SGFDxErrorCode;
import SecuGen.FDxSDKPro.jni.SGFDxSecurityLevel;
import SecuGen.FDxSDKPro.jni.SGFingerInfo;
import SecuGen.FDxSDKPro.jni.SGFingerPosition;
import SecuGen.FDxSDKPro.jni.SGImpressionType;
import SecuGen.FDxSDKPro.jni.SGPPPortAddr;
```

2.3 El API de Secugen para reconocimiento dactilar.

SecuGen FDxSDKPro es una librería para el reconocimiento de la huella dactilar incluido en el SDK, permitiendo integrar la biometría con los Applets desarrollados.

A continuación se describe el API que conforma SecuGen FDxSDKPro para el desarrollo de aplicaciones usando la biometría [28].

- **JSGFPLib**.- Es la clase principal que permite el acceso al dispositivo y brinda las funcionalidades del algoritmo.
- **SGFingerInfo**.- Permite obtener información del dispositivo SecuGen conectado.
- **SGFDxErrorCode**.- Permite manejar los mensajes de error que pueden ocurrir con SecuGen FDxSDKPro.
- **SGFingerPosition**.- Contiene la posición de las huellas dactilares utilizados durante el desarrollo.
- **SGFDxSecurityLevel**.- Contiene los valores de los niveles de seguridad se pueden utilizar al momento de utilizar el algoritmo.
- **SGDxDeviceName**.- Permite identificar los dispositivos SecuGen compatibles con esta librería.
- **SGPPPortAddr**.- Identifica el puerto que es utilizado por el dispositivo para enseguida reconocerlo.

2.4 Descripción del Applets de Registro de Huella Dactilar y del Applet de Verificación de Huella Dactilar

2.4.1 Métodos Utilizados para el Registro de la Huella Dactilar

Se agregó los siguientes objetos y variables para la captura de la huella dactilar.

TABLA VIII. VARIABLES PARA EL REGISTRO DE HUELLA.

```
//Variables a utilizar para el registro de la huella dactilar
    //Identifica tipo de dispositivo
    private long informaPuerto;
    //Para identificar el puerto del disp.
    private long puerto;
    //Primera Captura Huella
    private final byte[] regMin1 = new byte[400];
    //Segunda Captura Huella
    private final byte[] regMin2 = new byte[400];
    //Obtener Imagen 1
    private BufferedImage imgRegistro1;
    //Obtener Imagen 2
    private BufferedImage imgRegistro2;
    //Fijar la calidad de la Huella
    private int CalidadImagen = 50;
    //Fijar el tiempo de captura
    private int SegundosCaptura = 50;
    //Informa puerto USB del dispositivo biométrico
    private long infPuerto;
```

En el proceso de registro se captura la huella dactilar para comprobar la calidad de la misma, si la calidad de la imagen es aceptable se extraen los puntos característicos para crear una plantilla que será almacenada en la base de datos (bdmoodle).

Los métodos de dicho proceso se muestran a continuación.

Se requiere de un método que se ejecuta para inicializar el SDK de SecuGen, y así comenzar con el proceso de captura y registro.

TABLA IX. MÉTODO DE INICIALIZACIÓN DE COMPONENTES PARA LA CAPTURA DE LA HUELLA.

```
public Registro() {
        encendidoDispo = false; //
        //Lista de los dedos
        this.dedos = new ArrayList<>();
        // carga lista de dedos desde la DB
        cargarDedos();
        //Inicializa los componentes del JApplet
        initComponents();
        //Inicializa el SDK de SecuGen
        libFp = new JSGFPLib();
```

```
        // Habilita los botones del JApplet
        habilitarControles();
        jButtonInitActionPerformed(null);

    }
```

Con los métodos Captura_1 y Captura_2 se obtiene una muestra del dedo seleccionado para un mayor grado de precisión en el algoritmo; estos métodos permitirán verificar que la huella sean lo suficientemente visibles para su posterior análisis con el algoritmo. Para determinar la calidad de la huella es necesario el ancho y largo de la imagen, un array donde se encuentra la imagen, un matriz donde se almacenara la calidad de la imagen, retornando dos valores true en caso de tener buena calidad o false en caso contrario, además presenta los mensajes de error en caso de una mala calidad de la imagen.

TABLA X. MÉTODO QUE PERMITE LA CAPTURA DE LA HUELLA.

```
vhuella = libFp.CreateTemplate(fingerInfo, imageBuffer1, regMin1);

                if (vhuella == SGFDxErrorCode.SGFDX_ERROR_NONE) {
                    this.jLabelStatus.setText("Primer Registro de
Imagen Capturada");
                    r1Captura = true;
                    //     this.enableRegisterAndVerifyControls();
                } else {
                    JOptionPane.showMessageDialog(null, "Error en la
creaci\u00f3n de Plantilla", "ERROR", JOptionPane.ERROR_MESSAGE);
                    this.jLabelStatus.setText("Error en la
creaci\u00f3n de Plantilla...!!!" + vhuella);

                }
```

Para el registro de la huella dactilar y su almacenamiento a la base de datos se usa el método Registro, donde se establece como primer paso un nivel de seguridad alto, luego se crea una plantilla con las dos imágenes de la huella dactilar y verifica que las huellas ingresadas coincidan para extraer los puntos característicos de la misma y determinar si la plantilla es aceptable para así continuar con el almacenamiento de la huella dactilar en la base de datos.

TABLA XI. MÉTODO PARA REGISTRAR LA HUELLA.

```
if (reg_huella == SGFDxErrorCode.SGFDX_ERROR_NONE) {
            matchScore[0] = 0;
            reg_huella = libFp.GetMatchingScore(regMin1,
regMin2, matchScore);

            if (reg_huella == SGFDxErrorCode.SGFDX_ERROR_NONE) {
                if (matched[0]) {
```

```
                    Long id = (long) 1;
                    if (usuarioId != null) {
                        id = Long.parseLong(usuarioId);

                    }
                    String dedo = (String)
jComboBoxDedos.getSelectedItem();
                    int pos = dedo.indexOf(":");
                    Integer dedoId =
Integer.parseInt(dedo.substring(0, pos));
                    if (existeHuella(dedoId, id) == false) {
                        guardarHuella();
                        this.limpiarCampos();
                        try {

getAppletContext().showDocument(new
URL("https://accesoevaluaciones.sytes.net/moodle/login/login.php
" + "?id=" + usuarioId));
                        } catch (Exception e) {
                        }
                    } else {
                        editarHuella(id, dedoId);
                        this.limpiarCampos();
                        try {

getAppletContext().showDocument(new
URL("https://accesoevaluaciones.sytes.net/moodle/login/login.php
" + "?id=" + usuarioId));
                            this.destroy();
                        } catch (Exception e) {
                        }
                    }
                } else {
                    JOptionPane.showMessageDialog(null,
"Registro Fallido, ingrese el mismo dedo para registrar",
"ERROR", JOptionPane.ERROR_MESSAGE);
                    this.jLabelStatus.setText("Registro
Fallido...!!!" + matchScore[0]);
                    this.limpiarCampos();

                                        }
```

2.4.2 Métodos Utilizados para la Verificación de la Huella Dactilar

El proceso de verificación consiste en extraer los datos característicos de la huella almacenada con la huella ingresada y de esta manera analizar que estas correspondan validando la identidad del usuario, caso contrario se niega el acceso a la plataforma virtual de aprendizaje Moodle.

Los métodos utilizados se presentan a continuación.

Se agregó los siguientes objetos y variables para el proceso de verificación de la huella dactilar.

TABLA XII. VARIABLES PARA LA VERIFICACIÓN DE HUELLA.

```
//Variables a utilizar para la verificación de la huella dactilar
    //Identifica tipo de dispositivo
    private long informaPuerto;
    //Para identificar el puerto del disp.
    private long puerto;
    //Captura de Huella
    private final byte[] vrfMin = new byte[400];
    //Obtener imagen
    private BufferedImage imgVerificacion;
    //Fijar la calidad de la Huella
    private int calidadImagen = 50;
    //Fijar el tiempo de captura
    private int segundosCaptura = 50;
    //Lista de dedos
    private List<String> dedos;
```

Se requiere de un método que se ejecuta para inicializar el SDK de SecuGen, y así poder comenzar con el proceso de captura y verificación.

TABLA XIII. MÉTODO DE INICIALIZACIÓN DE COMPONENTES PARA LA CAPTURA DE LA HUELLA.

```
public Verificacion() {

          encendidoDispo = false;
          //Lista de los dedos
         this.dedos = new ArrayList<>();
         // carga lista de dedos desde la DB
         cargarDedos();
         //Inicializa los componentes del JApplet
         initComponents();
         // Habilita los botones del JApplet
         habilitarControles();
         jButtonInitActionPerformed(null);

    }
```

Para el proceso de la verificación se requiere tener una buena calidad de imagen de la huella usando el método captura_ 1 detallado en el punto **2.3.1 Métodos Utilizados para el Registro de la Huella Dactilar**, se define el nivel de seguridad como el más alto con el fin de minimizar las posibilidades de falsa aceptación (FAR). Se extraen los puntos característicos de la huella formando una plantilla y se los compara con la primera y segunda plantilla almacenada en la base de datos (bdmoodle). En caso de una verificación fallida no podrá tener acceso a la Plataforma Moodle, garantizando así la seguridad en la autenticación.

TABLA XIV. MÉTODO PARA LA VERIFICACIÓN DE LA HUELLA.

```
Verificacion c = new Verificacion();
            Connection cn = c.conectar();
             Statement stmt = cn.createStatement();
             String dedo = (String)
jComboBoxDedos.getSelectedItem();
             int pos = dedo.indexOf(":");
             Integer dedoId = Integer.parseInt(dedo.substring(0,
pos));
             ResultSet rs = stmt.executeQuery("SELECT * FROM
huella WHERE usuario_id =" + usuarioId + "  AND  dedo_id=" +
dedoId);
             if (rs.first()) {
                 //   if (rs.next()) {
                 System.out.println("Ingresa Primera Vez");
                 //Lee captura1 de la base de datos
                 byte templateHuella[] = rs.getBytes("captura1");
                 //Lee captura2 de la base de datos
                 byte templateHuella2[] =
rs.getBytes("captura2");

                 iError = fplib.MatchTemplate(templateHuella,
vrfMin, nivelSeguridad, matched);

                 if (iError == SGFDxErrorCode.SGFDX_ERROR_NONE) {
                     if (matched[0]) {
                         //Verificacion con Huella 1
                         verificacionHuella = true;
                         comprueba(verificacionHuella);
                         JOptionPane.showMessageDialog(null,
"Verificaci\u00f3n con \u00c9xito.");

                     } else {
                         verificacionHuella = false;
                         comprueba(verificacionHuella);
                         JOptionPane.showMessageDialog(null,
"Intento de Verificaci\u00f3n Fallido", "ERROR",
JOptionPane.ERROR_MESSAGE);
                         this.jLabelStatus.setText("Intento de
Verificaci\u00f3n  Fallido...!!!: " + iError);

                         this.limpiarCampos();
                                         }
```

2.5 Integración del Sistema de Reconocimiento de Huella Dactilar a la Plataforma Virtual Moodle.

La Plataforma Virtual de Aprendizaje Moodle, puede ser utilizado para grandes o pequeñas cantidades de usuarios; para el primer caso habitualmente se separa el servidor de la base de datos del servidor web, sin embargo esto no hará falta ya que

probaremos la Autenticación por Huella Dactilar a Moodle mediante pruebas piloto; con un pequeño número de huellas, pudiendo utilizar así un solo ordenador como servidor.

Antes de la integración del Sistema de Reconocimiento de Huella Dactilar es necesario e importante definir el tipo de autenticación a utilizar en la Plataforma Virtual Moodle.

2.5.1 Autenticación en Moodle

Una parte importante de la plataforma Moodle es la autenticación de los usuarios; es decir la manera en que cada uno de los usuarios se loguean al sitio (usuario y contraseña).

Moodle permite tener varios tipos de autenticación, entre los usados se encuentran:

- Manual
- Email
- LDAP
- IMAP
- POP3

A continuación se detalla los tres primeros tipos de autenticación de manera resumida.

2.5.1.1 Manual.

En la autenticación manual es el Administrador del sitio quien crea las cuentas de los usuarios, con nombre de usuario y claves para todos los integrantes.

2.5.1.2 Basada en Email.

Es el tipo de autenticación utilizado en el presente Trabajo de Titulación. En este tipo de autenticación el administrador permite a cada uno de los usuarios la creación de la cuenta para el ingreso a la plataforma Moodle de manera personal, como se realiza dicho proceso en diversos sitios y portales conocidos.

El requisito fundamental para este tipo de autenticación es configurar y habilitar la opción de Servidor de Email (Ver Anexo 2.1: Configuración del Servidor Email para la Plataforma Moodle), lo que permitirá a la plataforma virtual enviar un mensaje de confirmación de solicitud al usuario.

2.5.1.3 LDAP.

LDAP permite a Moodle conectarse a un Servidor de Dominios (LDAP), en el cual se almacena información de cada usuario basados en una estructura organizacional.

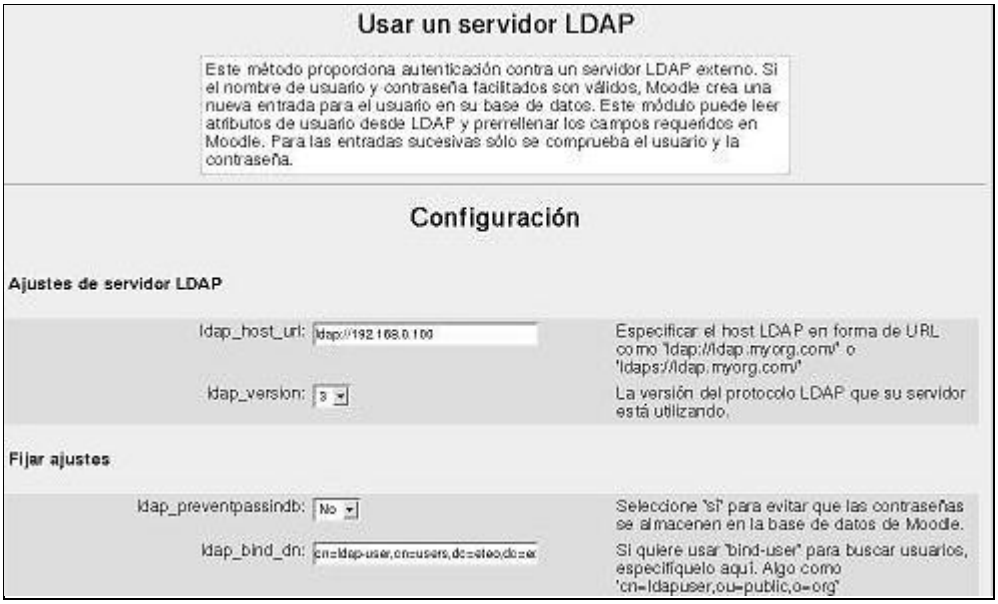


Figura 16. Creación de un Servidor LDAP.

2.6 Configuración y Creación de archivos de Moodle.

Los archivos que se crearon para el registro y la verificación en la autenticación mediante la huella dactilar son:

- **Login.php**.- El código de este archivo permite recuperar el ID del usuario cuando esté llena los campos de **Nombre de Usuario** y **Contraseña**.

TABLA XV. ARCHIVO LOGIN.PHP

```php
<?php
require('../config.php');
require_once('lib.php');
$id=$_GET["id"];
$user = $DB->get_record('user', array('id'=>$id));
//inicia sesión de usuario
complete_user_login($user);
$urltogo=$CFG->wwwroot.'/';
 redirect($urltogo);

?>
```

- **Huella.php**.- Realiza una consulta a la base de datos donde verifica que el ID recuperado con el archivo *Login.php* exista en la tabla **huella**, devolviendo verdadero si el usuario tiene guardada una huella dactilar o falso en caso de no tener una huella almacenada.

TABLA XVI. ARCHIVO HUELLA.PHP

```php
<?php
function tieneHuella($id){
$servername = "localhost";
$username = "usermoodle";
$password = "MoodleUser";
$dbname = "bdmoodle";
$resultado=false;

// Create connection
$conn = new mysqli($servername, $username, $password, $dbname);
// Check connection
if ($conn->connect_error) {
     die("Connection failed: " . $conn->connect_error);
}

$sql = "SELECT id FROM huella where usuario_id=".$id;
$result = $conn->query($sql);

if ($result->num_rows > 0) {
    $resultado=true;
} else {
   $resultado=false;
}
$conn->close();
return  $resultado;
}

?>
```

- **RegistroHuella.php.-** Este archivo permite incrustar el applet *Registro Huella* dentro de Moodle, extrae el ID del usuario como referencia para que sea almacenado junto con la huella dactilar procesada por el applet.

TABLA XVII. ARCHIVO REGISTROHUELLA.PHP

```php
<?php
require('../config.php');
require_once('lib.php');
$id=$USER->id;
require_logout();
echo    '<applet
```

```
  code     = "applet.RegistroHuella.class"
  name     = "RegistroHuella"
   archive  = "RegistroHuella.jar"
  width    = "400"
  height   = "530"
  hspace   = "0"
  vspace   = "0"
  align    = "middle"
>
<PARAM NAME="id" VALUE="'.$id.'">
</applet>';
?>
</center>

</body>
```

- **VerificacionHuella.php.-** Este archivo incrusta el Applet *VerificacionHuella* dentro de Moodle, extrae el ID del usuario como referencia para que sea almacenado junto con la huella dactilar procesada por el Applet.

TABLA XVIII. ARCHIVO VERIFICACIONHUELLA.PHP

```
<?php
require('../../config.php');
require_once('../lib.php');
$frm = false;

echo    '<applet
  code     = "applet.VerificacionHuella.class"
  name     = "VerificacionHuella"
   archive  = "VerificacionHuella.jar"
  width    = "400"
  height   = "530"
  hspace   = "0"
  vspace   = "0"
  align    = "middle"
>
<PARAM NAME="id" VALUE="'.$USER->id.'">
</applet>';
?>
</center>
          </body>
```

- **CerrarSesion.php.-** el código de este archivo permite regresar a la página principal cuando los datos del usuario como huella, nombre de usuario o contraseña son incorrectos.

TABLA XIX. ARCHIVO CERRARSESION.PHP

```php
<?php
require('../../config.php');
require_once('../lib.php');
require_logout();
header( 'Location:http://accesoevaluaciones.sytes.net/moodle' ) ;

 ?>
```

- **seguridad.php**.- este archivo se ejecuta invisiblemente al ojo del usuario abre automáticamente la cámara, presenta el mensaje para capturar la imagen, la procesa y la envía el archivo *guardar_foto.php*.

TABLA XX. SEGURIDAD.PHP

```
<script>

$(function() {

var cxt = canvas.getContext("2d");
canvas = document.getElementById("canvas");
video = document.getElementById("video");
                                                    if
(!navigator.getUserMedia)

navigator.getUserMedia = navigator.webkitGetUserMedia ||
navigator.mozGetUserMedia || navigator.msGetUserMedia;
                                                     if
(!window.URL)

window.URL = window.webkitURL;
                                                    if
(navigator.getUserMedia) {

navigator.getUserMedia({"video": true, "audio": false
}, function(stream) {

video.src = window.URL.createObjectURL(stream);

video.play();
}, function(err) {
console.log("Ocurrió el siguiente error: " + err); });
}else {
alert("getUserMedia no disponible");

return; }
// Evento click para capturar una foto.

video.addEventListener('loadedmetadata', function(e) {
                                                        var
relation = e.target.videoWidth / e.target.videoHeight;
```

```
canvas.width = 300;

canvas.height = 300 / relation;
                                                                    },
false);
// Evento click para enviar la foto al servidor.

$("#enviar").click(function() {

cxt.drawImage(video, 0, 0, canvas.width, canvas.height);
var data = canvas.toDataURL("image/jpeg");
// Separamos el ""
var info = data.split(",", 2);

$.ajax({ type: "POST", url: "guardar_foto.php", data: {

type: info[0],

data: info[1] },

success: function(result) {

console.log("result:", result);

                                                                    }
```

- **guardar_foto.php.-** permite decodificar la imagen, relacionar con el id del usuario, y almacenarla en un archivo dentro del servidor.

TABLA XXI. GUARDAR_FOTO.PHP

```
      <?php
require('../../config.php');
require('../lib.php');
$jpg = base64_decode($_POST["data"]);
$id_foto=date('YmdHis');
$id=$USER->id;
$file = fopen("fotos/foto".$id.".jpg", "w");


if($file){
        // Debe tener permiso de escritura.
      fwrite($file, $jpg);
      fclose($file);
      echo "ok";
         Response.End;
}
else{
      echo "Error al abrir archivo";} ?>
```

- **discapacidad.php.-** permite identificar si el usuario tiene o no discapacidad.

TABLA XXII. DISCAPACIDAD.PHP

```
$sql = "SELECT id FROM mdl_user_info_data WHERE DATA='SI' AND
userid=".$id;
$result = $conn->query($sql);
```

Se requiere también modificar ciertos archivos detallados a continuación:

- **index.php.-** Si el usuario tiene huella se invoca el Applet de Verificación, caso contrario se invoca al Applet de Registro.

TABLA XXIII. INDEX.PHP

```
if(tieneDiscapacidad($USER->id)){
                    unset($SESSION->loginerrormsg);
}else{
// Discard any errors before the last redirect.
  unset($SESSION->loginerrormsg);

//Si cuenta esta bloqueada salir caso contrario verificar huella

if(bloqueoCuenta($USER->id)){
$urltogo=$CFG->wwwroot.'/user/registrar/bloquearCta.php';
// test the session actually works by redirecting to self
            }else{

            if(tieneHuella($USER->id)){
            $urltogo=$CFG-
>wwwroot.'/user/verificar/verificacion.php';
            }else{
            $urltogo=$CFG-
>wwwroot.'/user/registrar/RegistroHuella.php';
            }}    }
```

- **confirm.php**. Presenta la acción del botón Registrar Huella, cuando el usuario desee modificar la huella dactilar registrada anteriormente.

TABLA XXIV. CONFIRM.PHP

```
//Presenta la acción del botón Registrar Huella

echo $OUTPUT->single_button("$CFG-
>wwwroot/user/RegistroHuella.php", get_string('Registrar
Huella'));
```

2.7 La Huella Dactilar en las Evaluaciones

Uno de los puntos importantes de nuestro Trabajo de Titulación es la integración de la huella dactilar dentro de los procesos de evaluación y de esta manera garantizar la identidad del usuario, quien ejecutará dicho proceso.

Antes de comenzar la evaluación es necesario verificar la identidad del usuario mediante la huella dactilar, para eso se ha modificado y creado los siguientes archivos:

- **VerificacionEvaluacion.-** Incrusta el Applet de Verificación de la Huella Dactilar enviando como parámetro el id del usuario y el id del parámetro que ejecuta la evaluación para la respectiva comparación.

TABLA XXV. VERIFICACION_EVALUACION.PHP

```
<?php
require('../../config.php');
require_once('../lib.php');
//original
$currentattemptid=$_GET['currentattemptid'];
echo    '<applet
  code     = "applet.VerificacionHuella.class"
  name     = "VerificacionHuella"
  archive  = "VerificacionHuella.jar"
  width    = "400"
  height   = "530"
  hspace   = "0"
  vspace   = "0"
  align    = "middle"
>
<PARAM NAME="currentattemptid" VALUE="'.$currentattemptid.'">
<PARAM NAME="id" VALUE="'.$USER->id.'">
</applet>';
?>
</center>
</body>
```

- **startattempt.php.-** Una vez que el usuario ha salido exitoso en la verificación de la huella dactilar se habilita la evaluación, cuya modificación se realiza en el archivo startattempt.php, que se encuentra por defecto en la carpeta de instalación de Moodle. Este archivo permite activar la evaluación a cada uno de los usuarios.

TABLA XXVI. STARTATTEMPT.PHP

```
if(tieneDiscapacidad($USER->id)){
redirect($quizobj->attempt_url($attempt->id, $page));
}else{
redirect(new
```

```
moodle_url('/user/verificar/verificacionEvaluacion.php',array('cur
rentattemptid'=>$attempt->id)));
}
```

- **attempt.php**. Permite capturar una imagen del usuario en un momento aleatorio durante la evaluación.

TABLA XXVII. ATTEMPT.PHP

```
if ($attemptobj->is_last_page($page)) {
    $nextpage = -1;
} else {
    $nextpage = $page + 1;

}if($page == 4){

      redirect(new moodle_url('/user/camara/seguridad.php'));
      }
```

- **VerificarEvaluacion.php.-** Habilita la evaluación en caso que la verificación con la huella dactilar se haya llevado a cabo correctamente.

TABLA XXVIII. VERIFICAR_EVALUACION.PHP

```
<?php
require('../../config.php');
$currentattemptid=$_GET['currentattemptid'];
 redirect(new
moodle_url("/mod/quiz/attempt.php?attempt=".$currentattemptid));
?>
```

2.8 Configuración de Tablas de la Base de Datos de Moodle.

Se muestra las tablas y relaciones necesarias para la base de datos bdmoodle, las mismas que son necesarias para el almacenamiento de la huella dactilar.

- **Nombre de la Base de Datos:** bdmoodle
- **Tablas creadas**

TABLA XXIX. TABLAS CREADAS

Nombre	Descripción
Huella	Almacena el identificador y la huella dactilar del usuario

Dedo	Almacena los tipos de dedos que puede ingresar el usuario
Intentos	Almacena los intentos realizados por el usuario durante la verificación de la huella.

- **Relaciones**: La tabla mdl_user es creada durante la instalación de Moodle. La relación entre las tablas dedo y huella indica que un dedo puede tener varias huellas y que a cada huella le corresponde un dedo. La relación entre las tablas huella y dedo muestra que un usuario tiene varias huellas dactilares y que una huella pertenece a una persona, como se observa en la Figura 17.

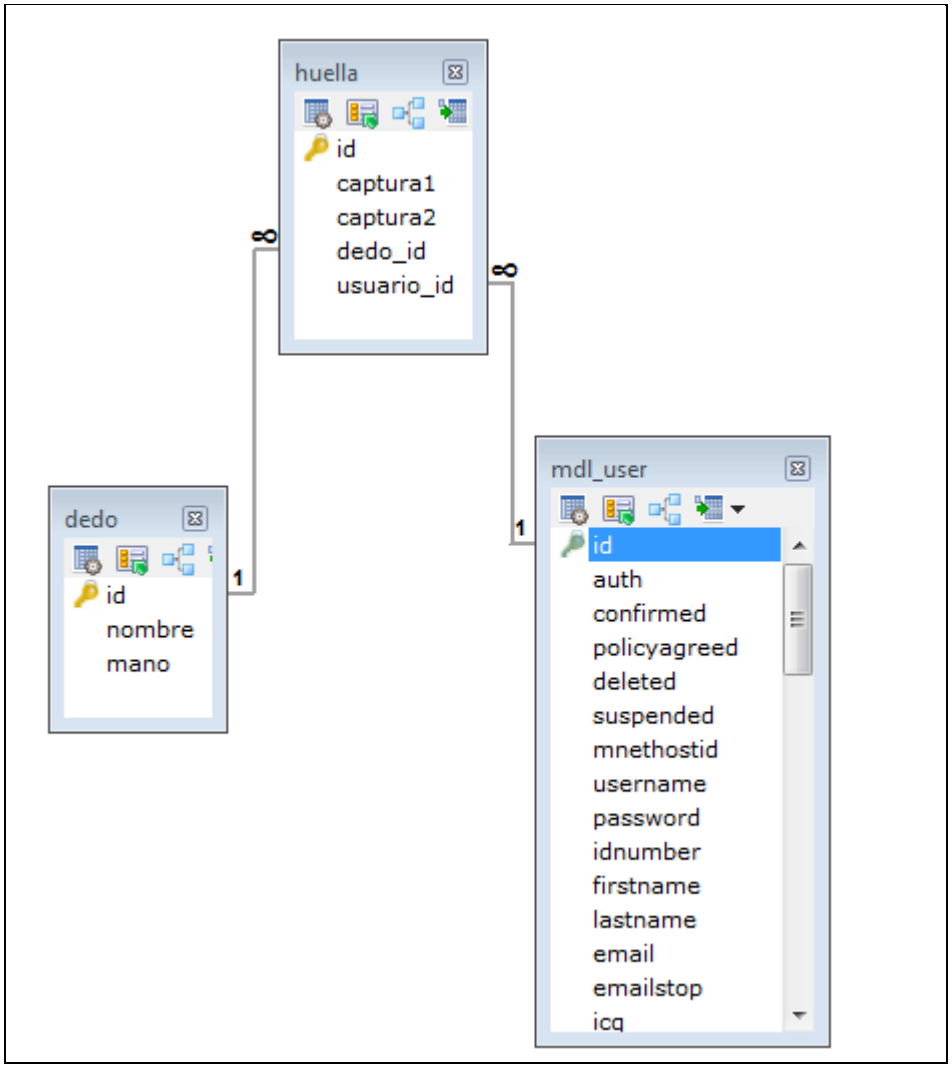


Figura 17. Configuración Base de Datos de Moodle.

- **Descripción de las tablas**

  TABLA DEDO: La columna ***ID*** almacena el identificador del dedo, la columna ***nombre*** indica el nombre del dedo y la columna ***mano*** indica la mano a la que pertenece el dedo.

  TABLA HUELLA: La columna ***ID*** indica el identificador de la huella dactilar las columnas ***captura_1*** y ***captura_2*** almacenan las huellas dactilares, la columna ***dedo_id*** almacena el identificador del dedo del que pertenece la huella dactilar y la columna ***usuario_id*** almacena el identificador del usuario al que pertenece la huella dactilar.

  TABLA MDL_INTENTOS: La columna **ID** almacena el identificador de los intentos, la columna **num_intentos** almacena el límite de los intentos realizados por el usuario en el proceso de verificación de la huella, la columna **fecha_bloqueo** almacena la fecha de bloqueo de la cuenta del usuario, la columna **id_usauario** almacena el identificador de cada usuario.

2.9 Funcionamiento del Sistema

La mayoría de los sistemas biométricos funcionan de maneras similares y se pueden resumir en dos pasos.

- **PASO 1:** El primer paso consiste en que el usuario debe registrarse en el sistema capturando el rasgo característico de la persona cuyo proceso será el siguiente.

Registro.- Para el registro de la huella dactilar existen dos casos: el auto registro de los alumnos y la creación manual de los usuarios. Para el primer caso cuando se crear la cuenta de usuario, se envía un mensaje de confirmación al correo ingresado, una vez confirmada la creación de la cuenta a se re direcciona al Applet de Registro Huella donde se registrara la huella dactilar del usuario; mientras que para el segundo caso el usuario ingresa con el nombre de usuario y clave asignada por el administrador, Moodle verifica si el campo huella dentro de la base de datos está lleno caso contrario muestra el Applet de Registro Huella.

En este proceso de inscripción la huella será leída por el dispositivo biométrico, el cual obtendrá dos muestras de los rasgos físicos de la huella dactilar, extrayendo la información adecuada para almacenarlas como plantillas dentro de la base de datos.

En la Figura 18 se puede observar el proceso de registro de los usuarios dentro de la plataforma Moodle.

Figura 18.- Registro de la Huella Dactilar.

- **PASO 2:** El segundo paso consiste en verificar la identidad del usuario cuyo proceso es el siguiente.

Verificación.- En el proceso de verificación se efectúa el reconocimiento de la identidad del usuario, donde se compara los rasgos biométricos con los de un patrón ya almacenado en la base de datos, este método es conocido con el nombre de uno para uno (1:1), lo que implica conocer hipotéticamente la identidad del usuario a autenticar. En la Figura 19 se puede observar el proceso de verificación de los usuarios dentro de la plataforma Moodle.

Figura 19.- Verificación de la Huella Dactilar.

Las evaluaciones especialmente en la educación a distancia son un factor determinante para medir el rendimiento de los estudiantes, por tal razón requieren de una técnica para poder minimizar la suplantación de identidad en el desarrollo de los mismos. El funcionamiento del sistema de la huella dactilar dentro del proceso de evaluación integrado a la plataforma virtual de aprendizaje como se puede observar en la Figura 20, comienza con la identificación del usuario al ingresar la evaluación, donde las características de la huella dactilar ingresada es comparada con la huella almacenada en la Base de Datos, en este proceso se desconoce la identidad, siendo así se debe de capturar una huella dactilar del usuario para que sea comparado por una huella registrada en la Base de Datos. Por medio de este proceso, se obtiene la identidad del individuo, en donde se obtiene un valor aceptado o rechazado verificando de esta manera si el usuario es o no quien realizará dicha evaluación, permitiendo minimizar la suplantación de los mismos durante dicho proceso.

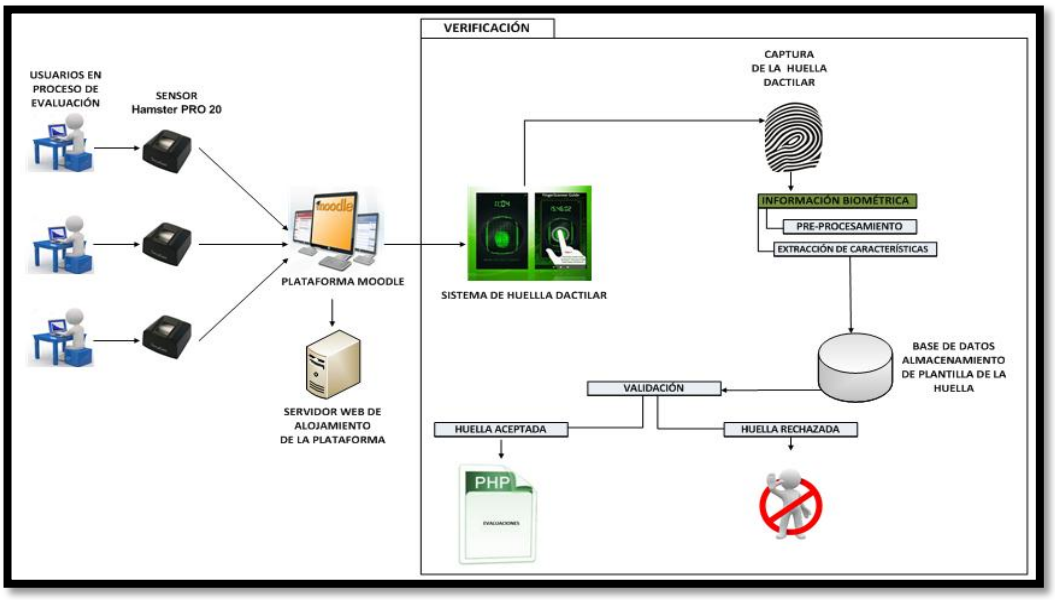


Figura 20.- Funcionamiento De La Huella Dactilar Procesos De Evaluación

La Figura 21 muestra el diagrama de flujo del proceso de autenticación biométrica dentro de la Plataforma Moodle

Diagrama de Flujo

Para una mejor comprensión del sistema se presenta el diagrama de flujo donde se indica cómo se llevan a cabo la operación de verificación y como se procesa la huella dactilar.

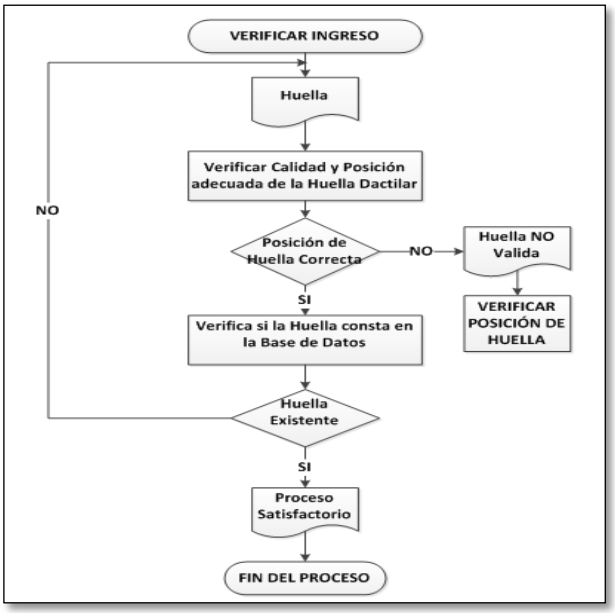


Figura 21.- Funcionamiento De La Huella Dactilar Procesos De Evaluación.

Fase 3: Emplear técnicas de seguridad de datos, que permitan asegurar la información recibida por la plataforma virtual.

Como solución a esto y para el cumplimiento de este objetivo se analiza métodos que permitan proteger el nombre de usuario, la clave y su huella dactilar que son usadas al momento de autenticarse en Moodle.

3.1. Estudio de métodos para la protección de datos.

Se ha realizado un análisis a los métodos que permitan dar seguridad a nivel de autenticación, siendo los siguientes:

- **Protocolo HTTPS:** El protocolo Seguro de Transferencia de Hipertexto HTTPS, es un canal de comunicaciones seguro que se utiliza para intercambiar información entre un equipo cliente y un servidor, mediante la utilización de certificados SSL, cuyo propósito es proporcionar seguridad a los datos que se utilizan vía internet. Este método de protección de los datos es muy importante, ya que permite que los datos que viajen a través del internet sean encriptados ante cualquier sustracción de información confidencial [31].

  HTTPS es un protocolo de capa aplicación cuyo puerto por defecto es el 443; en sí decimos que es una implementación de HTTP que brinda seguridad en la transferencia de datos dentro de una red insegura o redes de acceso público.

  El protocolo HTTPS es muy empleado en lugares que requieren que sus datos sean seguros ante cualquier eventualidad como instituciones bancarias o cualquier sistema que maneja la información sensible de cada uno de sus usuarios.

  El funcionamiento del protocolo HTTPS comienza cuando el usuario se conecta a un servidor con implementación HTTPS, donde se obtiene un certificado digital, el cual es generado mediante certificados seguros SSL, de no ser así el navegador genera una alerta indicando que dicho sitio no es seguro [31].

  En la conexión se realiza cifrado de datos, por tal razón HTTPS emplea protocolos SSL/TSP, para crear un canal seguro de transferencia de datos.

  El manejo de certificados consta de dos claves una pública y una privada. La clave pública es la utilizada por los clientes para poder desencriptar la información

recibida, mientras la clave privada es empleada por el servidor para encriptar la información y así mantenerla segura.

- **ReCaptcha:** El captcha es un tipo de medida de seguridad conocido como autenticación pregunta-respuesta, que ayuda a protegerse del spam y del descifrado de contraseñas mediante el acceso remoto de otros ordenadores no autorizados. Este método de protección permite determinar que personas no autorizadas o con una entidad falsa tengan ingreso y saturen el servidor al contar con usuarios falsos.

- **Antivirus:** El antivirus ClamAV software Open Source, es empleado por la plataforma virtual de aprendizaje Moodle cuyo propósito es analizar los archivos que se suben al servidor, evitando la inserción de virus o cualquier archivo nocivo que atente la información contenida en el servidor.

- **Encriptación de Plantillas:** Muchos de los dispositivos biométricos para garantizar que los datos ingresados sean seguros, proporcionan librerías que permiten que estos datos sean encriptados, permitiendo que la información no sea alterada, modificada o manipulada por personas no autorizadas para beneficio de los mismos.

  SecuGen Pro 20, lector de huellas dactilar proporciona plantillas encriptadas que garantiza que las huellas ingresadas se mantengan seguras ante cualquier eventualidad y garantizar que los datos ingresados por cada uno de los usuarios estén seguros y protegidos.

3.2. Selección y aplicación de métodos de protección de datos aplicados a la información de los usuarios en la Plataforma Virtual de Aprendizaje

Para garantizar la seguridad en la autenticación del usuario se ha seleccionado y configurado todos los mecanismos antes mencionados. La configuración se la realiza de la siguiente manera.

3.2.1. Protocolo HTTPS (Hypertext Transfer Protocol Secure).

Se usa el protocolo HTTPS para proteger la información que viaja a través del internet durante el proceso de acceso, así mismo se hace uso de los certificados digitales para garantizar la autenticidad en la parte del servidor y el cliente y sirven para implementar el protocolo HTTPS.

3.2.1.1. Creación de los certificados digitales.

Para obtener un certificado digital es conveniente adquirirlo a una entidad autorizada para la emisión de los mismos, sin embargo se utilizará el módulo openssl, incluido en apache 2.4, dicho módulo sirve para crear estos certificados y firmarlos de manera personal.

El certificado que se crea posee el mismo nivel de encriptación que cualquier certificado emitido por una entidad autorizada, con la diferencia de que no aparecen en las listas de los navegadores.

Antes de crear los certificados digitales es necesario copiar el archivo openssl.cnf desde *C:\server\Apache24\conf* a *C:\server\Apache24\bin.*

Para la creación de los certificados digitales dirigirse al directorio *C:\server\Apache24\bin*, utilizando el CMD de Windows se seguirán los siguientes pasos.

Paso 1:

Ejecutar el siguiente comando:

- *openssl req -config openssl.cnf -new -out biometrico.csr -keyout biometrico.pem*

Se solicitara la siguiente información para el certificado:

- **Enter PEM pass phrase:** contraseña segura.
- **Country Name (2 letter code) [AU]:** EC.
- **State or Province Name (full name) [Some-State]:** Loja.
- **Locality Name (eg, city) []:** Loja.
- **Organization Name (eg. company)[Internet Widgits Pty Ltd]:** UNL.
- **Organization Unit Name:** CIS

- **Common Name (eg. Server FQDN or YOUR name) []:** accesoevaluaciones.sytes.net.
- **Email Address []:** mariatroya90@gmail.com.

La información que se considera obligatoria es la clave privada PEM y Common Name que el nombre del dominio a asegurar.

Paso 2:

Ejecutar este comando para crear el archivo .key que contiene la llave privada del certificado digital.

- *openssl rsa -in biometrico.pem -out biometrico.key*

Paso 3:

Finalmente se ejecuta el siguiente comando para crear el certificado X.509 que también requiere Apache.

- *openssl x509 -in biometrico.csr -out biometrico.cert -req -signkey biometrico.key -days 365.*

Luego de haber seguido los pasos mencionado se tendrá creado el certificado digital denominado **biométrico**, finalmente se copia los archivos del certificado a la carpeta conf de Apache en este caso ubicado en C:\server\Apache24\conf.

3.2.1.2. Configuración de Apache para el uso de certificados digitales.

Los archivos a configurar son httpd.conf y ssl.conf a continuación se explica la modificación realizada a cada uno de los archivos.

3.2.1.3. Configuraciones archivo httpd.conf.

Habilitar el modulo SSL de Apache des comentando las siguientes líneas:

- *LoadModule socache_shmcb_module modules/mod_socache_shmcb.so*
- *LoadModule ssl_module modules/mod_ssl.so*
- *Include conf/extra/httpd-ssl.conf*

3.2.1.4. Configuraciones archivo ssl.conf.

Ubicamos las direcciones de los certificados digitales creados anteriormente:

- *SSLCertificateFile "c:/server/Apache24/conf/biometrico.cert"*
- *SSLCertificateKeyFile "c:/server/Apache24/conf/biometrico.key"*

3.2.2. Creación de Hosting Virtual en servidor Apache.

El Hosting Virtual nos permite configurar las conexiones https.

Para habilitar el servicio HTTPS (443) se requiere editar el archivo ssl.conf de la siguiente manera:

- Des comentar la opción de escucha del puerto 443.
- Agregar la dirección donde está instalado Moodle en la línea de DocumentRoot.
- Aumentar el nombre del dominio del servidor virtual y el puerto de escucha.
- Agregar la dirección de los certificados digitales.

Quedando de la siguiente manera.

TABLA XXX. HOSTING VIRTUAL PARA HTTPS

```
<VirtualHost _default_:443>
    ServerAdmin mariatroya90@gmail.com
    DocumentRoot "c:/server/Apache24/htdocs"
    ServerName accesoevaluaciones.sytes.net:443
    ErrorLog "c:/server/Apache24/logs/error.log"
    TransferLog "c:/server/Apache24/logs/access.log"

    SSLEngine on

    SSLCertificateFile "c:/server/Apache24/conf/biometrico.cert"
    SSLCertificateKeyFile "c:/server/Apache24/conf/biometrico.key"

<Directory "c:/server/Apache24/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>

</VirtualHost>
```

3.2.3. Configuración de la Plataforma Moodle para usar autenticación segura.

Una vez realizada la configuración del protocolo HTTPS en el servidor Apache es necesario configurar Moodle para que acepte dicho protocolo.

Mediante la sesión de Administrador de Moodle se activa la función de autenticación segura mediante HTTPS como indica la Figura 22. Los pasos a seguir son:

- Ingresar al bloque de **Administración**
- Seleccionar la opción de **Seguridad**
- Elegir **Seguridad HTTP**
- Activar la opción **Usar HTTPS para accesos**

  Finalmente Guardar los cambios realizados.

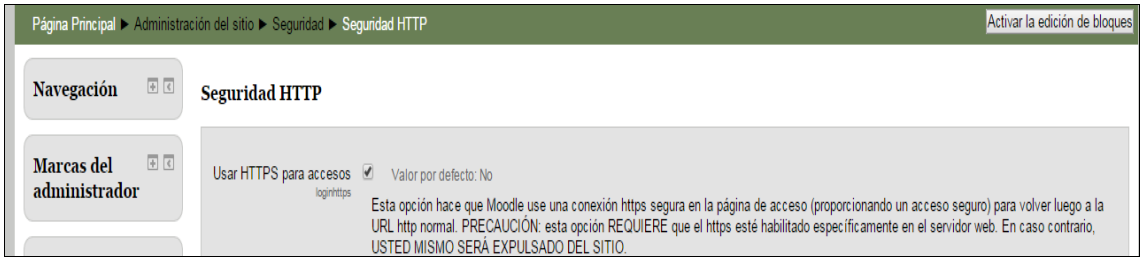


Figura 22.- Configuración de Moodle para autenticación segura.

3.3. Uso de reCatpcha en el registro de usuario.

Los métodos de autenticación de cada uno de los usuarios pueden ser diversos dentro de la plataforma virtual de aprendizaje Moodle, ya sea utilizando plugins compatibles con la plataforma o mediante la autenticación por defecto. Tomando en cuenta la seguridad de acceso a la plataforma Moodle sea implementado un método de seguridad en el registro de cada uno de los usuarios llamado CAPTCHA, cuya función es la de autentificar la identidad de una persona al darse de alta en una web.

El CAPTCHA puede considerase también como una medida de seguridad conocido como autenticación pregunta-respuesta, que ayuda a protegerse del spam o también conocido correo no deseado, además del descifrado de contraseñas. La seguridad CAPTCHA ofrece protección contra entradas remotas, que hace que un ser humano con la contraseña correcta pueda acceder.

La implementación del CAPTCHA dentro de la plataforma Moodle permite evitar las entradas no autorizadas en dichas cuentas, garantizando la protección de la información de cada uno de los usuarios, además de reforzar la seguridad en los puntos de acceso a las cuentas más sensibles.

Para insertar un CAPTCHA en la plataforma es necesario registrase en la página oficial: *http://www.recaptcha.net/*, una vez registrados nos proporcionaran dos claves: una clave pública para generar un plugin en el formulario de registro de la plataforma, y una clave privada para la comunicación entre Moodle y el servidor CAPTCHA (ver Figura 23).

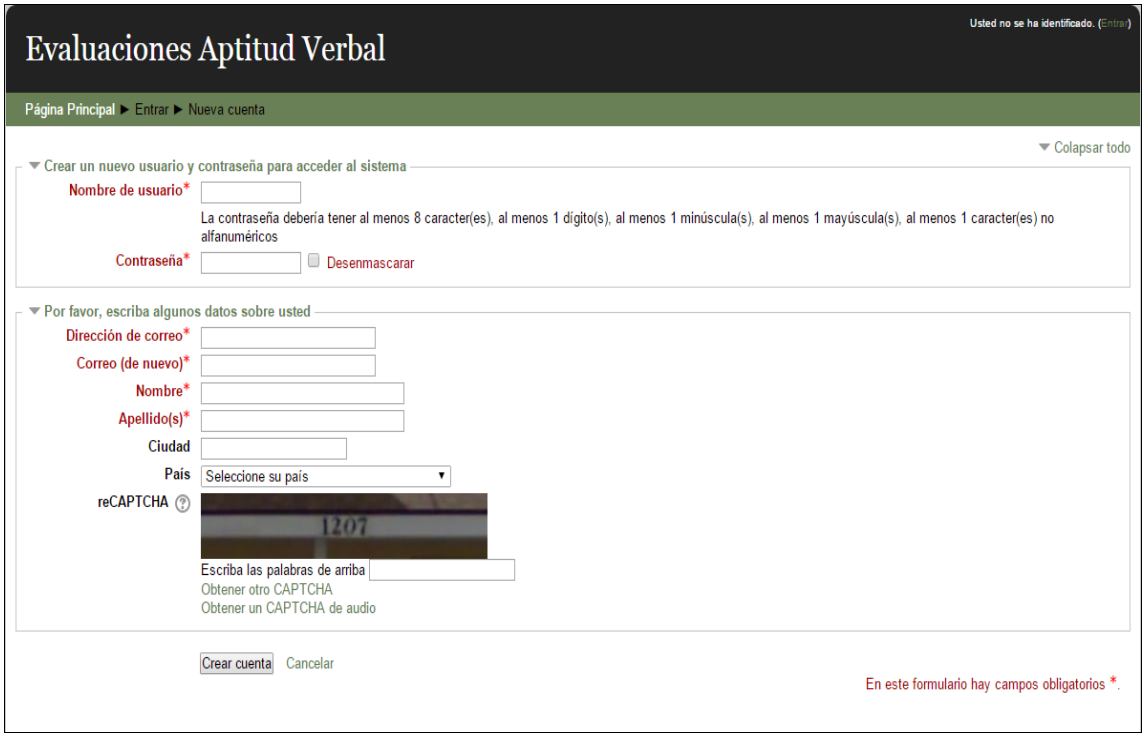


Figura 23. Implementación del CAPTCHA (Moodle).

El funcionamiento de un CAPTCHA consta de una secuencia de letras o de números generados de forma aleatoria mediante una imagen y un cuadro de texto.

Fase 4: Evaluar el correcto funcionamiento del sistema mediante pruebas piloto.

El objetivo del presente Trabajo de Titulación no es la implementación del sistema, sino la presentación de una propuesta para minimizar la suplantación de identidad, utilizando un sistema biométrico para la autenticación y en el proceso de evaluaciones, razón por la cual es necesario validar la funcionalidad de la Plataforma.

4.1. Pruebas de funcionamiento y fiabilidad del sistema en la Plataforma Virtual de Aprendizaje

Para realizar las pruebas de funcionamiento y fiabilidad de la huella dactilar se ha puesto en marcha la Plataforma Virtual de Aprendizaje Moodle en un servidor de modo que sea accesible desde internet, permitiendo obtener resultados del registro y verificación de la huella dactilar, además se creó un curso con una actividad única como es el cuestionario denominado Aptitud Verbal, para obtener resultados de la verificación dentro de los procesos de evaluación.

4.1.1. Permitir que Moodle sea accesible desde cualquier IP, para lograrlo se requiere:

- Un servicio de redirección DNS que para estas pruebas se ha utilizado el servicio No-Ip que permite convertir la IP dinámica a estática pero teniendo un nombre de dominio.
- Desde el router utilizado redireccionar el trafico HTTP, y HTTPS hacia el servidor Web.
    - En el archivo *C:\server\Apache24\htdocs\moodle\config.php* cambiar el valor de la variable $CFG->wwwroot quedando de la siguiente manera:
      $CFG->wwwroot = 'http://'.$_SERVER["HTTP_HOST"].'/moodle';

4.1.2. Evaluación de Resultados

Para la validación de las pruebas de funcionamiento y fiabilidad de la huella dactilar se usa las siguientes tasas.

FAR (False Acceptance Rate) Tasa de Falsa Aceptación. Indica que una huella no registrada ingrese al sistema [17].

FRR (False Rejection Rate) Tasa de Falso Rechazo. Indica que una huella registrada en el sistema sea rechazada [17].

Se usaron 50 huellas dactilares diferentes para los procesos de registro, verificación en la autenticación y verificación en la evaluación, en total se obtuvo 150 capturas de huellas dactilares de las cuales:

- 126 capturas fueron identificadas correctamente.
- 15 capturas no pudieron ser identificadas por el Sistema.
- 9 capturas no pudieron ser procesadas por la baja calidad que presentaba la huella.

Las huellas que no son tomadas en cuenta para el cálculo y análisis de las tasas son las 9 huellas que no fueron permitidas, ya sea por la baja calidad que presentaban o por la mala posición del dedo a la hora de la captura, siendo así se han tomado en cuenta 141 de las 150 huellas capturadas. Cabe recalcar que las 9 huellas que no fueron procesadas en la primera vez, tuvieron que volver a ser capturadas nuevamente de modo para que todos los usuarios puedan dar la evaluación.

Los resultados obtenidos en el registro, verificación en la autenticación y verificación en la evaluación se muestran en la TABLA XXXI.

TABLA XXXI. INFORME DE PRUEBAS

USUARIO	***PROCESOS***		
	Registro	*Verificación en Autenticación*	*Verificación en Evaluación*
usuario1	ACEPTADA	ACEPTADA	ACEPTADA
usuario2	ACEPTADA	ACEPTADA	ACEPTADA
usuario3	ACEPTADA	NO IDENTIFICADAS	ACEPTADA
usuario4	ACEPTADA	ACEPTADA	ACEPTADA
usuario5	ACEPTADA	ACEPTADA	ACEPTADA
usuario6	ACEPTADA	ACEPTADA	ACEPTADA
usuario7	NO PROCESADA	ACEPTADA	NO IDENTIFICADAS
usuario8	ACEPTADA	NO IDENTIFICADAS	ACEPTADA
usuario9	ACEPTADA	ACEPTADA	ACEPTADA
usuario10	NO PROCESADA	ACEPTADA	ACEPTADA
usuario11	ACEPTADA	ACEPTADA	ACEPTADA
usuario12	NO PROCESADA	ACEPTADA	ACEPTADA
usuario13	ACEPTADA	NO IDENTIFICADAS	ACEPTADA
usuario14	ACEPTADA	NO IDENTIFICADAS	ACEPTADA
usuario15	ACEPTADA	ACEPTADA	ACEPTADA

usuario16	ACEPTADA	ACEPTADA	ACEPTADA
usuario17	ACEPTADA	ACEPTADA	NO IDENTIFICADAS
usuario18	ACEPTADA	ACEPTADA	ACEPTADA
usuario19	ACEPTADA	ACEPTADA	ACEPTADA
usuario20	ACEPTADA	ACEPTADA	ACEPTADA
usuario21	NO PROCESADA	ACEPTADA	ACEPTADA
usuario22	ACEPTADA	NO IDENTIFICADAS	ACEPTADA
usuario23	ACEPTADA	ACEPTADA	ACEPTADA
usuario24	ACEPTADA	ACEPTADA	ACEPTADA
usuario25	ACEPTADA	ACEPTADA	ACEPTADA
usuario26	ACEPTADA	ACEPTADA	ACEPTADA
usuario27	ACEPTADA	ACEPTADA	ACEPTADA
usuario28	ACEPTADA	ACEPTADA	ACEPTADA
usuario29	NO PROCESADA	ACEPTADA	ACEPTADA
usuario30	NO PROCESADA	ACEPTADA	ACEPTADA
usuario31	ACEPTADA	ACEPTADA	ACEPTADA
usuario32	ACEPTADA	ACEPTADA	ACEPTADA
usuario33	ACEPTADA	ACEPTADA	ACEPTADA
usuario34	ACEPTADA	ACEPTADA	ACEPTADA
usuario35	NO PROCESADA	NO IDENTIFICADAS	ACEPTADA
usuario36	ACEPTADA	ACEPTADA	ACEPTADA
usuario37	ACEPTADA	NO IDENTIFICADAS	ACEPTADA
usuario38	ACEPTADA	ACEPTADA	ACEPTADA
usuario39	ACEPTADA	ACEPTADA	ACEPTADA
usuario40	NO PROCESADA	ACEPTADA	ACEPTADA
usuario41	ACEPTADA	ACEPTADA	NO IDENTIFICADAS
usuario42	ACEPTADA	ACEPTADA	ACEPTADA
usuario43	ACEPTADA	ACEPTADA	ACEPTADA
usuario44	ACEPTADA	ACEPTADA	NO IDENTIFICADAS
usuario45	ACEPTADA	ACEPTADA	ACEPTADA
usuario46	NO PROCESADA	NO IDENTIFICADAS	ACEPTADA
usuario47	ACEPTADA	ACEPTADA	NO IDENTIFICADAS
usuario48	ACEPTADA	ACEPTADA	ACEPTADA
usuario49	ACEPTADA	NO IDENTIFICADAS	ACEPTADA
usuario50	ACEPTADA	ACEPTADA	NO IDENTIFICADAS

Considerando las 141 huellas que fueron procesadas correctamente se obtuvieron los siguientes resultados.

$$FAR = \frac{falsas\ aceptaciones}{total\ de\ huellas\ procesadas} x100\%$$

$$FAR = \frac{0}{141} x100\% = 0\%$$

$$FRR = \frac{falsas\ rechazos}{total\ de\ huellas\ procesadas} x100\%$$

$$FRR = \frac{9}{141} x100\% = 6.38\%$$

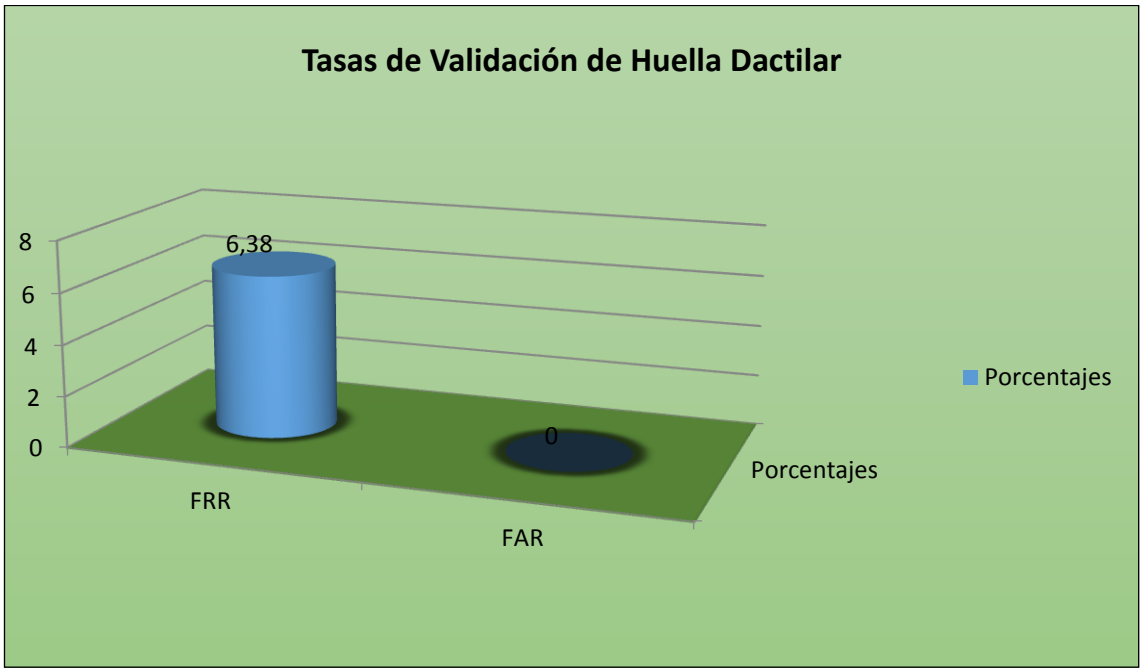


Figura 24. Tasas de Validación de Huella Dactilar

Los resultados presentados son bueno, ya que los valores de la Tasa de Falsas Aceptaciones es realmente nulo, lo cual significa que al Sistema no puede ingresar una huella dactilar que no ha sido registrada, mientras que la Tasa de Falsos Rechazos es un valor realmente muy bajo, indicando que una mínima cantidad de huellas procesadas son rechazadas, de estos resultados podemos concluir que el sistema es confiable en la identificación de las huellas dactilares (ver Figura 24).

4.2. Identificación de errores tanto técnicos como lógicos

Durante la interacción con la plataforma se pudieron detectar los siguientes errores:

- Se ha detectado que se ingresa a la cuenta de un usuario sin registrar la huella dactilar, cuando se copia el Url de la sesión en el navegador.
- Cuando se abre el Applet de Registro en un navegador no se puede volver abrir el Applet de Verificación debido a que ambos Applets usan la librería jnisgfplib.dll teniendo el usuario que cerrar y volver abrir el navegador, es decir los dos Applets no pueden ejecutarse en dentro de la JVM.

4.3. Corrección de errores

Los resultados de esta prueba fueron utilizados para modificar y agregar mejoras a la Plataforma con el fin de corregir los problemas. Cabe recalcar que no fue necesario hacer cambios significativos.

Para solucionar el acceso sin registrar la huella dactilar se ha creado el archivo *CerrarSession.php* que es invocado desde el Applet de Registro cuando el usuario intenta acceder a la cuenta sin antes registrar su Huella Dactilar.

TABLA XXXII. CERRAR_SESSION.PHP

```
<?php
require('../../config.php');
require_once('../lib.php');
require_logout();
header( 'Location:http://accesoevaluaciones.sytes.net/moodle'
) ;
?>
```

Para la solución de librerías se ha hecho uso del método propio de los Applets **destroy(),** que es invocado después que se ha verificado la huella dactilar o después del registro para liberar la librería jnisgfplib.dll.

Con el mismo fin se ha agregado el parámetro *<Param name = "separate_jvm" = "true">* en el Applet de Registro y en el de Verificación para que estos se ejecuten en su propia instancia del JVM, sin que haya interferencia entre estos.

c. Discusión

La implementación de sistemas biométricos ha permitido automatizar los procesos de reconocimiento de identidad, de manera que pueden ser aplicados a mejorar los procesos de seguridad, siendo así, la biometría se ha convertido en un elemento clave en cuanto a técnicas de identificación. Por tal razón la técnica la huella dactilar aplicada especialmente en la educación trata de minimizar la suplantación de identidad para poder obtener credibilidad en las mismas y mejor la calidad de educación.

Para la implantación del presente proyecto se ha podido determinar cada una de las evidencias obtenidas en los objetivos explicados a continuación:

1. Desarrollo de la propuesta alternativa.

- **OBJETIVO 1: Comparar y seleccionar tecnologías biométricas, que se adapten dentro de una plataforma virtual de aprendizaje.**

Para el cumplimiento de este objetivo se ha revisado fuentes de información, estudios, artículos científicos y/o trabajos relacionados que contienen información útil referente a las tecnologías biométricas de reconocimiento de identidad, permitiendo así realizar un análisis de las diferentes tecnologías biométricas, en relación a sus ventajas, desventajas, así como las tendencias futuras.

Así mismo se han revisado ejemplo sobre implantaciones de biometría aplicada a Plataformas Virtuales de Aprendizaje, identificando y analizando el proceso de integración y los beneficios que han aportado estas implantaciones.

- **OBJETIVO 2: Integrar el sistema de autenticación a la Plataforma Virtual de Aprendizaje (Moodle).**

Para el cumplimiento de este objetivo se desarrolló un sistema de autenticación por huella dactilar utilizando Applets, que facilitaron la integración dentro de la plataforma Moodle, mediante el paso de parámetros, como el id del usuario que sirvió para el registro y verificación de cada uno de los mismos. Dentro de esta fase se crearon archivos necesarios para la autenticación biométrica así mismo se configuro archivos en la carpeta de instalación de Moodle, para el proceso

de autenticación y procesos de evaluación impartidos en la plataforma de aprendizaje de Moodle.

En este objetivo se utilizó como tecnología biométrica el sensor Hamster PRO 20, cuyo dispositivo permitió la captura de cada una de las huellas de los usuarios.

- **OBJETIVO 3: Emplear técnicas de seguridad de datos, que permitan asegurar la información recibida por la plataforma virtual.**

Dentro de este objetivo se empleó técnicas de seguridad de datos, mediante el empleo de plantillas de huella encriptados, las mismas que son propias de las librerías del dispositivo, además se creó un servidor propio para garantizar la protección de las bases de datos, mediante el acceso con certificados SSL que permiten que el mismo sitio sea seguro y encriptado, permitiendo garantizar que los datos sean protegidos ante cualquier amenaza de robo de los mismos.

Para el cumplimiento de este objetivo también se empleó dentro de la autenticación de ingreso de los estudiantes el re-captcha siendo esta una medida de seguridad conocido como autenticación pregunta-respuesta, que ayuda a protegerse del spam y del descifrado de contraseñas mediante el acceso remoto de otros ordenadores no autorizados [32].

Por tal razón dentro de esta fase, el objetivo es que los datos utilizados en la plataforma, sean protegidos ante cualquier eventualidad que pueda suceder.

- **OBJETIVO 4: Evaluar el correcto funcionamiento del sistema mediante pruebas piloto.**

Una de las etapas del ciclo de vida de cualquier proceso es evaluar el correcto funcionamiento del sistema, por tal razón el objetivo de esta fase es verificar el sistema mediante la aplicación de pruebas piloto para la evaluación del sistema, y de esta manera poder identificar errores tanto técnicos como lógicos que se puedan ver en la evaluación del mismo, y de esta manera poder corregirlos para que cumplan los requerimientos deseados.

Una vez finalizadas las etapas correspondientes al presente Trabajo de Titulación, se documentan y exponen las conclusiones alcanzadas en el informe final.

2. Valoración técnica económica ambiental.

El desarrollo del presente trabajo implicó una inversión económica, ya exigió recursos que se dedicaron en gran medida alcanzar los objetos planteados, los cuales se materializan a través de acciones basadas en un plan lógico, el cual correspondió con costos que se especifican a continuación:

TABLA XXXIII. RECURSOS HUMANOS

Rol	Número de Horas	Precio/Hora ($)	Valor Total ($)
María Troya	400	5.00	2000.00
Darío Bravo	400	5.00	2000.00
Asesor	30	0.00	0.00
		SUBTOTAL 1 ($)	**4000.00**

TABLA XXXIV. RECURSOS TÉCNICOS

Descripción	Cantidad	Valor Unitario ($)	Valor Total ($)	Depreciación Anual ($)
Hardware				
Computador	2	800.00	1600.00	533.33
Impresora	1	100.00	100.00	33.33
Disco Externo	1	120.00	120.00	40.00
Dispositivo biométrico SECUGEN	1	130.00	130.00	43.33

Software				
Látex	2	00.00	00.00	00.00
Open Proyect	1	00.00	00.00	00.00
Moodle	2	00.00	00.00	00.00
			SUBTOTAL 2 ($)	**649.99**

TABLA XXXV. RECURSOS MATERIALES

Descripción	**Cantidad**	**Valor Unitario ($)**	**Valor Total ($)**
Cartuchos de tinta	4	25.00	100.00
Resma de papel	1	4.00	4.00
Transporte	200	0.25	50.00
Internet	500h	0.80	400.00
Copias	200	0.02	4.00
Varios		50.00	50.00
		Subtotal 3 ($)	**608.00**

TABLA XXXVI. COSTE TOTAL DE RECURSOS

Recurso	**Subtotal ($)**
R. Humano	4000.00
R. Técnico	649.99
R. Material	608.00
Subtotal	**5257.99**
Imprevistos (5%)	262.89
Total	**5520.88**

d. Conclusiones

De los resultados obtenidos en la implementación de la plataforma mediante pruebas piloto se puede determinar las siguientes conclusiones:

- Dentro de los múltiples sistemas de reconocimiento biométrico se escogió al sistema biométrico de reconocimiento de huella dactilar como una alternativa de seguridad adicional para el acceso a la plataforma, minimizando el riesgo de suplantación de identidad.
- Emplear técnicas de seguridad de datos, permite minimizar el robo de los mismos, garantizando que cualquier proceso se pueda efectuar con una mayor confiabilidad.
- Entre varios sistemas biométricos el sistema de huella dactilar es el que se considera el más confiable con un margen de error del 0.01%.
- Los sistemas biométricos permiten la identificación y verificación de la identidad de las personas basándose en diferentes características, sin embargo ninguno se considera 100% confiable.
- Emplear técnicas biométricas como medidas de seguridad permite minimizar la suplantación de identidad, al poseer rasgos únicos de cada persona.

e. Recomendaciones

Una vez desarrollado el presente proyecto y puesto en marcha mediante pruebas piloto se han podido determinar las siguientes recomendaciones.

- Antes de iniciar la aplicación de verificación de identidad para el acceso a la plataforma se recomienda verificar que el dispositivo a usar sea compatible con el sistema desarrollado y se encuentre correctamente instalado.
- Cuando se registra la huella dactilar en la base de datos es recomendable verificar que dicha huella sea lo más clara posible para una correcta verificación a futuro.
- Aunque la elección del dedo a usar es de elección del usuario se recomienda usar el dedo pulgar, ya que además de ser el más cómodo es el que presenta características más fiables.
- Realizar un estudio profundo a las diferentes técnicas biométricas de manera que se pueda utilizar la combinación de dos o más de técnicas con el fin de eliminar la suplantación de identidad al momento de ingresar a la Plataforma Moodle.
- Para garantizar el correcto funcionamiento de la captura de la huella, debemos tomar en cuenta la posición correcta de la huella en lector.
- Para la seguridad en la Plataforma Virtual de Aprendizaje, se recomienda adquirir certificados digitales a una entidad autorizada, para así evitar problemas de acceso al usuario y garantizar la validez del sitio web.
- Para la implementación del sistema se recomienda usar equipos (servidores, red de alta velocidad) adecuados para el desempeño y eficiencia del mismo.

f. Bibliografía

Referencias Bibliográficas

[1] (2014, Abril) Acerca de Moodle. [Online]. http://docs.moodle.org/all/es/Acerca_de_Moodle

[2] (2013, Marzo) Manuales de Moodle, Unidad Informática y Comunicaciones, Universidad Luterana Salvadoreña. [Online]. http://www.uls.edu.sv/pdf/manuales_moodle/queesmoodle.pdf

[3] C. Belloch. (2012, Diciembre) Entornos Virtuales de Formación. [Online]. http://www.uv.es/bellochc/pedagogia/EVA9.wiki?3

[4] J. Toro N. Lopez, "Técnicas de Biometría Basada en Patrones Faciales del Ser Humano," UNIVERSIDAD TECNOLOGICA DE PEREIRA, Colombia, Tesis 2012.

[5] M. Aguilera, "Reconocimiento Biométrico Basado en Imágenes de Huellas Palmares," Universidad Autónoma de Madrid, Madrid, Tesis 2012.

[6] J. Landi, "Introducción a la biometría informática y análisis de la huella dactilar como fuentes de autenticación en sistemas de seguridad," Universidad Politécnica Salesiana Cuenca, Cuenca, Tesis 2007.

[7] J. García Garrigos, "Sistema de Autenticación Biométrica de Huella Dactilar asistido por Interfaz de Voz para el Control de Accesos," Universidad de Valencia, Valencia, Proyecto Fin de Carrera 2012.

[8] C. Hernadez Garces and R. Martínez, "Análisis de un Sistema de Autenticación por huella Dactilar para Fotalecer el Sistema de Seguridad para Utilizar el Software de la Empresa Farmaceuticos.," *Teoría General de los Sistemas*, vol. 1, pp. 4-5, 2013.

[9] E. Álvarez, S. De la Fuente, L. García, and C. Gutiérrez P. Peréz, "Estudio sobre las tecnologías biométricas aplicadas a la seguridad," pp. 1-100, Diciembre 2011.

[10] T. Areito J. Areito, "Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación," Universidad del País Vasco, País Vasco, Artículo 2010.

[11] S. León, "Avances En Técnicas Biométricas Y Sus Aplicaciones En Seguridad," Universidad Nacional Abierta, Venezuela, Artículo 2011.

[12] Vicerrectorado de Investigación, "Biometría Capacidades de I+D, soluciones tecnológicas y empresas UPM". Informe realizado por el Área de Innovación, Comercialización y Creación de Empresas," Universidad Politécnica de Madrid, Madrid, Artículo s.f.

[13] J. Chavéz D. Blanco, "Sistema de Reconocimiento Facial Utilizando el Análisis de Componentes Principales con una Red Neuronal BackPropagation Desarrollada en C++ y Matlab," Universidad Politécnica Salesiana, Quito, Tesis 2012.

[14] L. Zamudio, "Reconocimiento del iris como identificación biométrica utilizando el video," Instituto Politécnico Nacional, Tijuana, Tesis 2010.

[15] L. Ponce Párraga, "Sistema de Información para el Control de Asistencia del Personal Administrativo y Docente de la FACCI, mediante la técnica biométria de Geometría de la Mano," Universidad Laica Eloy Alfaro , Manabí, Tesis 2010.

[16] A. Czajka, "Template Ageing in Iris Recognition," *Biometrics Compendium, IEEE*, vol. 1, pp. 2-5, Mayo 2013.

[17] V. Hidalgo Jácome, "Implementación de un Sistema de Autenticación Biométrica Basado en Huellas Digitales," Escuela Superior Politécnica de Chimborazo, Riobamba, Tesis 2010.

[18] J. Feng and Nandakumar A. K. Jain, "Fingerprint Matching," *Computer*, vol. 43, pp. 36-44, 2010.

[19] M. Rodriguez, J. Franco J. Mite, "Sistema de Control y Gestión de Personal para Pymes," Escuela Superior Politécnica del Litoral, Guayaquil, Tesis (s.f).

[20] M. Zapata, "Evaluación de competencias en entornos virtuales de aprendizaje y docencia universitaria," Universidad de Alcalá, Madrid, Madrid, pp. 18-19 (s.a).

[21] M. Castro, G. Diaz, E. Ruiz, A. Martín and S. Martín R. Gil, "Sistema de Verificación por Huella Dactilar en Exámenes en Moodle," *IEEE-RITA*, vol. 7, pp. 37-44, Febrero 2012.

[22] P. Gaona García J. Lopéz Vargas, "Vulnerabilidades sobre Mecanismos de Seguridad en Plataformas LCMS Open Source a Nivel de Autenticación," *Entérese*, vol. 1, pp. 75-85, Diciembre 2009.

[23] E. San Cristóbal, M. Tawfik,S. Martín, A. Pesquera, G. Díaz, A. Colmenar, J. Carpio, J. Peire and M. Castro R. Gil, "Aplicaciones y Seguridad en la Implementación de Competencias Prácticas en Entornos de Gestión de Aprendizaje," *ARBOR*, vol. 187, pp. 137-141, Diciembre 2011.

[24] M. Castro, G. Díaz, S. Martín and E. Ruiz R. Gil, "Nuevo Modelo de Evaluación Asistida por Ordenador en Educación a Distancia," *RIED*, vol. 15:2, pp. 143-170, 2012.

[25] Forero Alejandro, "Análisis de la Implementación de Huellas Dactilares y Firmas Digitales en los Registros de un Software de Historia Clínica Electrónica en Colombia," *Global Information Assurance Certification Paper*, p. 14, Abril 2010.

[26] Juan Garcia, "Accesos, Sistema de Autenticación Biométrica de Huella Dactilar Asistido por Interfaz de Voz Para el Control de," Universidad de Valencia, España, Proyecto Fin de Carrera 2011.

[27] (2014, Marzo) Manual PHP. [Online]. http://www.php.net/manual/es/intro-whatis.php

[28] K. Mohammed, *la biblia del servidor Apache*, Segunda ed., V. Ruiz, Ed. Madrid, España: ANAYA MULTIMEDIA, 2002.

[29] SecuGen Corporation. (2014) Secugen Biometrics Solutions. [Online]. http://www.secugen.com/products/hamster-pro-20.htm

[30] Oracle. (2014) JAVA. [Online]. https://www.java.com/es/download/faq/whatis_java.xml

[31] O. Belmonte Fernández, "Introducción al lenguaje de programación Java," Universitat Jaume, España , 2010.

[32] B. Rivadeneira, "Análisis y Diseño de una Solución Informática que Garantice alta Disponibilidad a los Servidores de Educacion Virtual," Escuela Politécnica Nacional, Quito, Tesis 2010.

[33] L. Romero, "La Seguridad Informática en el Trabajo con la Plataforma Moodle," *Revista de Humanidades*, vol. I, p. 22, Noviembre 2010.

[34] Griaule Biometrics. (2014) Fingerprint SDk. [Online]. http://www.griaulebiometrics.com/page/es/fingerprint_sdk

g. Anexos

Anexo 1: Especificaciones Técnicas del Dispositivo Biométrico SecuGen.

Nombre (Modelo)	Hamster Pro 20 (HU20 ™)
Sensor óptico de huellas dactilares	Sub-20 ™
Resolución de la imagen	500 DPI
Tamaño de la imagen	300 x 400 píxeles
Tamaño de platina	18,2 mm x 22,9 mm
A partir del área de detección	15,24 mm x 20,32 mm
Velocidad de captura de huellas dactilares	0,2 ~ 0,5 segundos con Smart Capture ™
Temperatura de funcionamiento	-20 ° ~ 65 ° C
Humedad de funcionamiento	90% o menos de humedad relativa, sin condensación
Dimensiones / Peso	31,6 x 58,5 x 53,9 mm / 98 g
Voltaje de la fuente / Max. Corriente	5 V DC / 150 Ma
Interfaz	USB 1.1 Full-Speed USB 2.0 de alta velocidad
Estándares soportados	ANSI INCITS 378, BioAPI, FIPS 201 y FAP 20 (PIV-071006) (Función de PDF), ISO / IEC 19794-2, ISO / IEC 19794-4, SP 800-76 (vista PDF)
Certificaciones	FCC, CE, RoHS, FBI (más información), GSA FIPS 201 APL (más información), STQC
Sistemas operativos compatibles	De Windows 8.1 / 8/7 / Vista / XP Windows Server 2012, 2008 R2, 2003 Java, Linux

Anexo 2: Instalación Componentes para Moodle

La instalación de Moodle se realizó de manera independiente para una mejor facilidad en la programación y modificación de cada uno de los archivos que requieren una modificación al integrar el sistema de huella dactilar a dicha plataforma.

A continuación se detalla la instalación de cada una de las herramientas que nos servirán para poner en marcha nuestra plataforma virtual de aprendizaje Moodle. Para la instalación se requiere del paquete de Moodle 2.6, el servidor Apache 2.4, un lenguaje de código abierto adecuado para el desarrollo web PHP 5.5.12, y el instalador del gestor de base de datos MySql 5.5, se encontrará en los siguientes enlaces dependiendo de la arquitectura de nuestra máquina ya sea x86 o x64:

Apache 2.4: http://httpd.apache.org/download.cgi

Php 5.5.12: http://windows.php.net/download/

MySql 5.5: http://dev.mysql.com/downloads/mysql/

Moodle: http://download.moodle.org/

Dado que estos paquetes (Apache) están compilados con Visual C++ para que sean compatibles con Windows, Debemos Tener instalado Visual C++ RedistributablePackage 2010 SP1.

Visual C++: http://www.microsoft.com/es-es/download/details.aspx?id=30679

Se debe de tener en cuenta que las versiones tanto del Apache como del PHP deberán ser CV11 ya que están optimizados para trabajar con PHP, y son compatibles entre sí.

Para que sea una instalación ordenada se creará una carpeta **server** en el disco C. donde instalaremos Apache, PHP, MySql, y Moodle.

INSTALACIÓN DE APACHE:

1. Dentro de la carpeta **server** se ubica el archivo descomprimido del servidor web **Apache 2.4**.

2. En el archivo **httpd.conf** situado en **C:\server\Apache24\conf\httpd.conf** configurar lo siguiente.

TABLA XXXVII. CONFIGURACIÓN APACHE

ServerRoot "c:/server/Apache24" *ServerName localhost:80* *DocumentRoot "c:/server/Apache24/htdocs"*

La primera instrucción define la ruta de instalación del servidor Apache, La segunda indica la el nombre de dominio al cual responderá el servidor seguido del puerto de escucha, la instrucción DocumentRoot indica la carpeta que contendrá las paginas html de PHP.

3. Una vez configurado el Apache, ingresamos al cmd la siguiente ruta para instalar Apache como un servicio: **C:\server\Apache24\bin,** para lo cual tecleamos el siguiente comando **httpd -k install .**

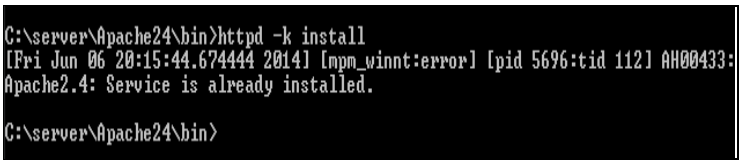


Figura 25. Instalación de Apache como Servicio

INSTALACIÓN DE PHP:

1. Ingresar al archivo httpd.conf, ubicado en la siguiente ruta: **C:\server\Apache24\conf\httpd.conf,** e ingresar las siguientes líneas de código.

TABLA XXXVIII. CÓDIGO CONECCIÓN APACHE CON PHP

```
LoadModule php5_module "C:/server/php/php5apache2_4.dll"
AddHandler application/x-httpd-php. php
#configure the path to php.ini
PHPInidir "C:/server/php"
```

2. Copiar el archivo de instalación descomprimido de PHP en la unidad C:\server\. Ubicarse en el archivo **php.ini-development,** ya que utilizaremos un ambiente de desarrollo, creamos un archivo con el nombre **php.ini** y pegamos el contenido.

3. Verificar que estén habilitadas las siguientes librerías de PHP como se muestra en la TABLA XXXIX.

TABLA XXXIX. EXTENCIONES PARA PHP

```
extension_dir = "./ext/"          >Sirve definir la carpeta con las extensiones .dll
extension=php_pdo_mysql.dll > para trabar como objetos las consultas sobre mysql
extensión=php_curl.dll          > para instalación de Moodle
extension=php_mysql.dll         > para cargar la antigua api de acceso a mysql
extension=php_mysqli.dll        > nueva y mejorada api de acceso a mysql
```

4. En la TABLA XL se muestra la configuración de los parámetros que permitirán el funcionamiento de Moodle.

TABLA XL. PARÁMETROS PARA FUNCIONAMIENTO DE MOODLE

```
[opcache]
opcache.enable = 1
opcache.memory_consumption = 128
opcache.max_accelerated_files = 4000
opcache.revalidate_freq = 60

opcache.use_cwd = 1
opcache.validate_timestamps = 1
opcache.save_comments = 1
opcache.enable_file_override = 0

[ExtensionList]
zend_extension=php_opcache.dll
extension=php_intl.dll
extension=php_intl.dll
```

5. Por último se configurara las directivas *intl.default_locale* y *intl.error_level* como se muestra en la TABLA XLI.

TABLA XLI. HABILITAR EXTENSIONES

```
[intl]
intl.default_locale = en_utf8
intl.error_level = E_WARNING
extension=php_soap.dll
extension=php_xmlrpc.dll
extension=php_openssl.dll
extension=php_mbstring.dll
extension=php_gd2.dll
```

INSTALACIÓN DE MYSQL:

1. Cuando se instala el gestor de base de datos MySQL, se cambia la ruta de instalación a **C:\server\mysql**.

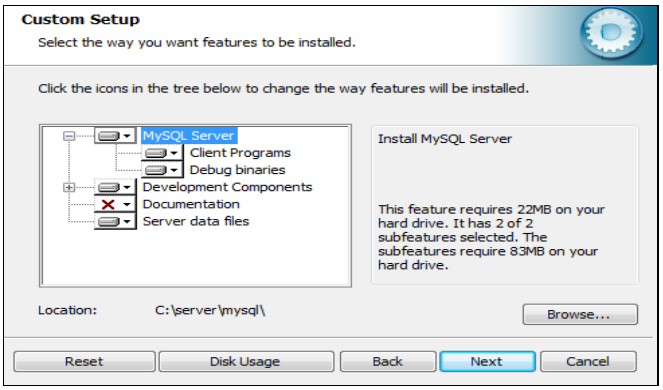


Figura 26. Asistente instalador MySQL

Se continúa con la instalación tradicional para el gestor de base de datos MySQL.

INSTALACIÓN DE MOODLE:

Antes de comenzar con la instalación de Moodle se debe de ingresar al cliente de MySQL, y crear una base de datos que la llamaremos **bdmoodle**, con los siguientes comandos

```
mysql> create database bdmoodle Default CHARSET utf8;
Query OK, 1 row affected (0.04 sec)

mysql> GRANT ALL PRIVILEGES ON bdmoodle.* TO 'usermoodle'@'localhost' IDENTIFIED
 BY "MoodleUser" WITH GRANT OPTION;
Query OK, 0 rows affected (0.05 sec)

mysql>
```

Figura 27. Creación de Base de Datos

Una vez creada la base de datos se descomprime el archivo .zip de instalación de Moodle en la ubicación **C:\server\Apache24\htdocs\moodle.**

1. Abrir en un navegador cualquiera la dirección **localhost/Moodle/install.php,** en la primera página que aparece se selecciona el idioma, y presionar **Siguiente**.

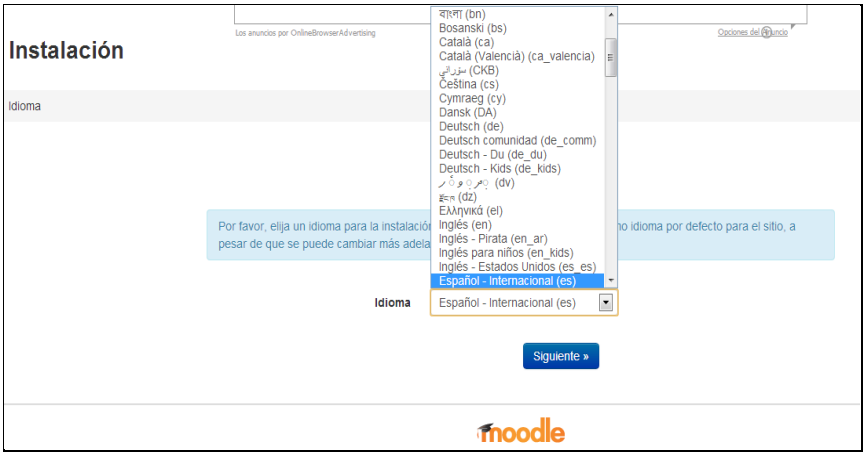


Figura 28. Elegir idioma de Moodle.

2. Confirmar rutas para la dirección Web y directorio de datos y presionamos **Siguiente** como se muestra en la Figura 29**.**

Figura 29. Confirmar rutas de directorio de Moodle.

3. Seleccionar el controlador del gestor de base de datos MySqL y presionar **Siguiente.**

Figura 30. Seleccionar controlador.

4. Se llena los campos creados en el gestor de base de datos MySql como se muestra a continuación y se selecciona **Siguiente.**

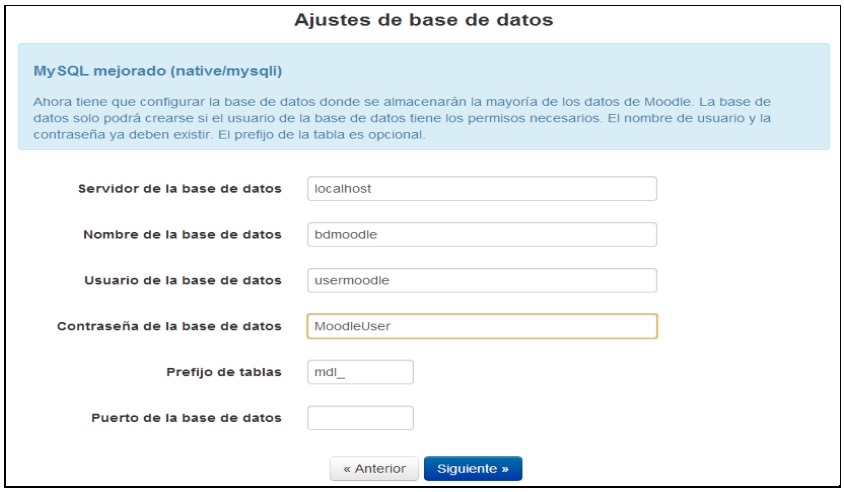


Figura 31. Ajustes de la Base de Datos.

5. Aceptar los términos de licencia y presionar **Continuar.**

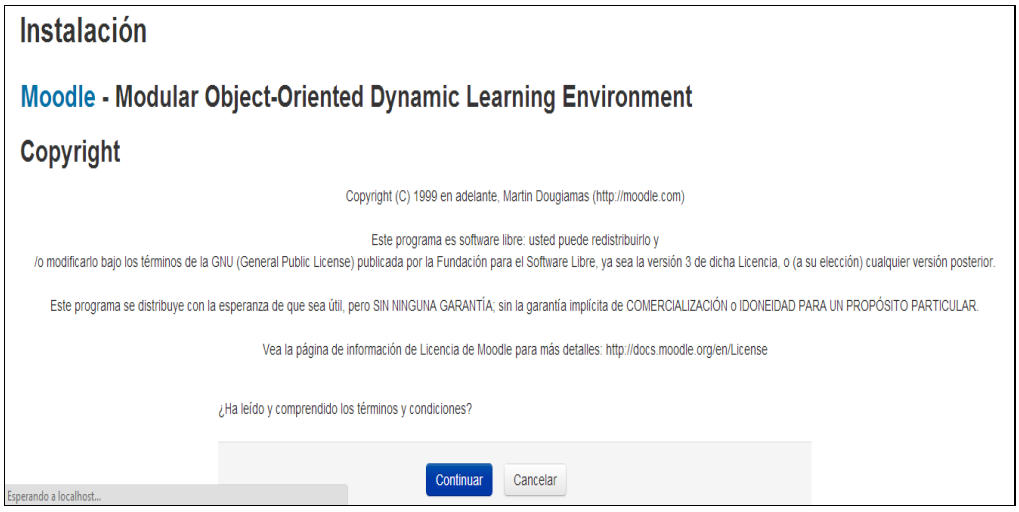
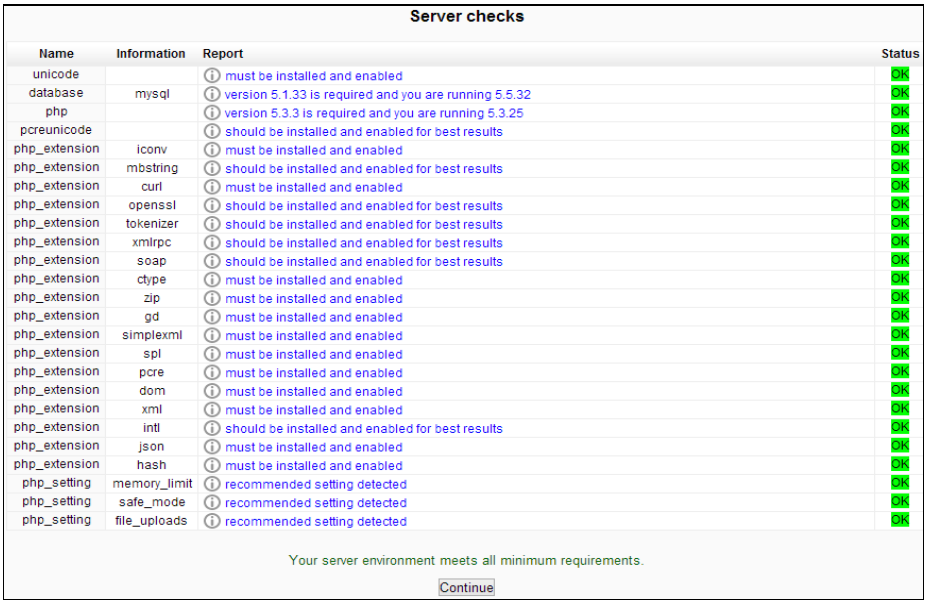


Figura 32. Términos de licencia.

6. Se presenta la siguiente página donde indica que todos los archivos php están correctamente configurados, y seleccionamos **Continuar.**



Server checks

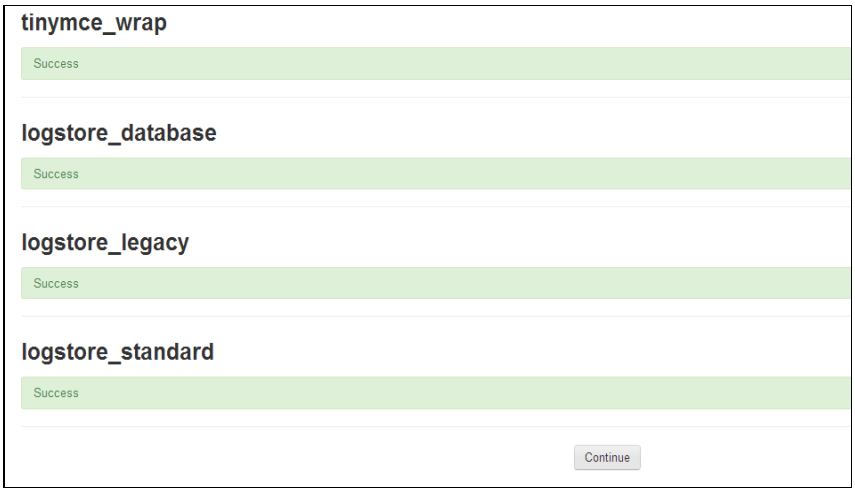
Name	Information	Report	Status
unicode		must be installed and enabled	OK
database	mysql	version 5.1.33 is required and you are running 5.5.32	OK
php		version 5.3.3 is required and you are running 5.3.25	OK
pcreunicode		should be installed and enabled for best results	OK
php_extension	iconv	must be installed and enabled	OK
php_extension	mbstring	should be installed and enabled for best results	OK
php_extension	curl	must be installed and enabled	OK
php_extension	openssl	should be installed and enabled for best results	OK
php_extension	tokenizer	should be installed and enabled for best results	OK
php_extension	xmlrpc	should be installed and enabled for best results	OK
php_extension	soap	should be installed and enabled for best results	OK
php_extension	ctype	must be installed and enabled	OK
php_extension	zip	must be installed and enabled	OK
php_extension	gd	must be installed and enabled	OK
php_extension	simplexml	must be installed and enabled	OK
php_extension	spl	must be installed and enabled	OK
php_extension	pcre	must be installed and enabled	OK
php_extension	dom	must be installed and enabled	OK
php_extension	xml	must be installed and enabled	OK
php_extension	intl	should be installed and enabled for best results	OK
php_extension	json	must be installed and enabled	OK
php_extension	hash	must be installed and enabled	OK
php_setting	memory_limit	recommended setting detected	OK
php_setting	safe_mode	recommended setting detected	OK
php_setting	file_uploads	recommended setting detected	OK

Your server environment meets all minimum requirements.

Continue

Figura 33. Archivos PHP.

7. En la Figura 34 se muestra como se instala cada uno de los componentes de Moodle y seleccionamos **Continuar.**



tinymce_wrap

Success

logstore_database

Success

logstore_legacy

Success

logstore_standard

Success

Continue

Figura 34. Componentes de Moodle.

8. A continuación se llena los campos donde vamos a ubicar el nombre del curso, contraseña de administrador, usuario, y otros datos que nos servirán para nuestra Página Moodle.

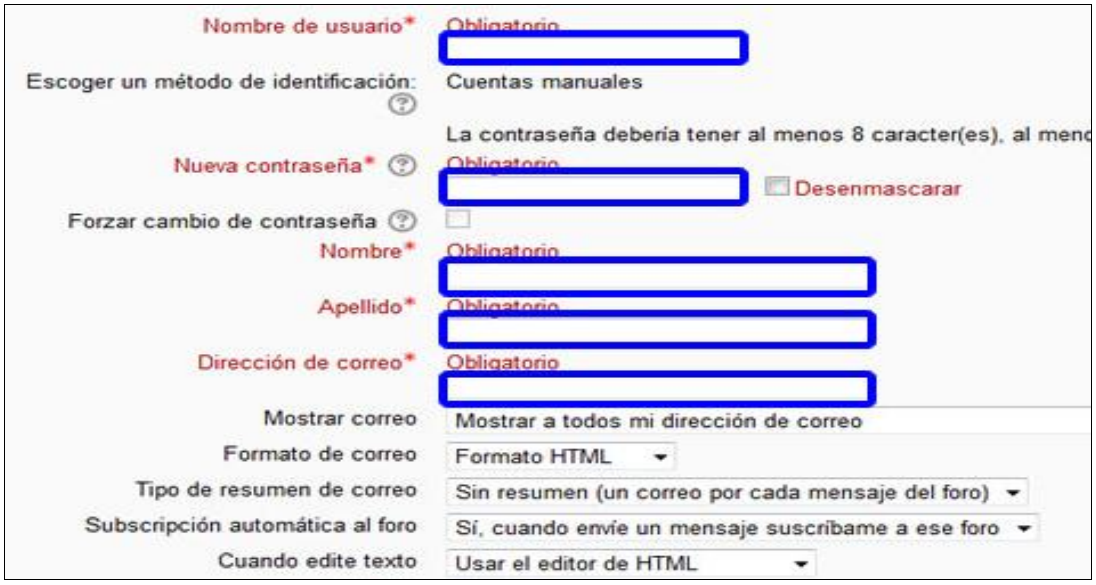


Figura 35. Información General de la Plataforma Moodle.

9. Una vez llenados los campos de Nuestra Página, seleccionamos actualización de página finalizando con la instalación de Moodle.

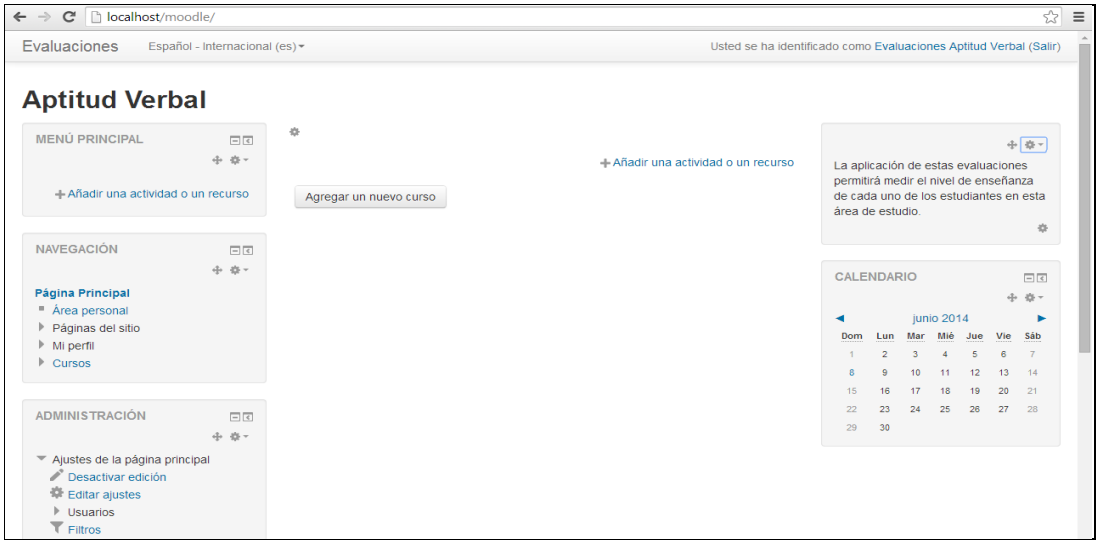


Figura 36. Plataforma Moodle.

Anexo 2.1: Configuración del Servidor Email para la Plataforma Moodle

En este apartado se definen las configuraciones competentes del uso adecuado del servidor y el funcionamiento del mismo. A continuación se describe los parámetros a configurar.

El Email permite configurar la conexión de la plataforma virtual hacia el servidor de correos el mismo que se encargará de enviar todos los mensajes generados como mensajería interna y registros de autenticación para cada uno de los usuarios que participen dentro de la plataforma.

Para la configuración de la funcionalidad del envío de mensajes se requiere los siguientes datos:

- Dirección IP del Servidor de Correos (SMTP).
- Cuenta de correo (nombre de usuario SMTP y contraseña).
- Definición de la hora del envío.
- Caracteres de codificación para el envío de mensajes, los cuales deben ser los que pertenecen al servidor.

Para ello hay que acceder a nuestra cuenta de administrador de Moodle y ubicarnos en lo siguiente:

Administración del Sitio → Extensiones → Mensajes de Salida →Email.

En la página de configuración del Email, habrá que introducir los siguientes parámetros y así configurar nuestro servidor SMTP.

Servidores SMTP: smtp.gmail.com:465
Seguridad SMTP: SSL
Nombre de usuario SMTP: Tu dirección de correo electrónico @ gmail.com o en su propio dominio.
Contraseña SMTP: contraseña de la cuenta de correo electrónico

En la Figura 37 se puede apreciar la configuración del Servidor SMTP de la plataforma Moodle.

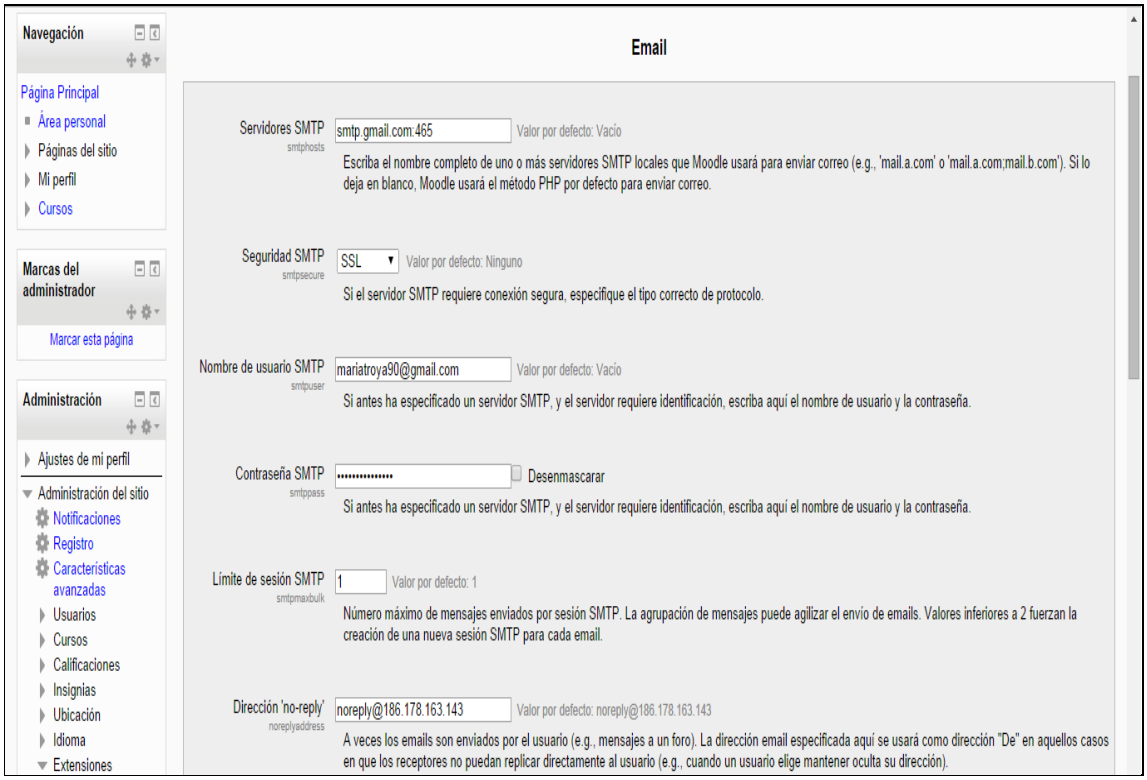


Figura 37. Configuraciones del Servidor SMTP.

Una vez introducido los campos antes explicados, pulsamos el botón Guardar en la parte inferior del formulario y de esta manera Moodle enviará notificaciones de ingreso a través de Email.

Anexo 3: Instalación de Componentes del Dispositivo Biométrico.

Anexo 3.1: Instalación y Configuración FDx SDK Pro for Windows v3.7_J14

La instalación de FDx SDK Pro for Windows v3.7 se lo realiza de la siguiente manera:

Ejecutar el archivo setup.exe del programa FDx SDK Pro for Windows v3.7 .

Figura 38. Instalador de FDx SDK

A continuación se presenta el asistente de instalación, seleccionar la opción **Next.**

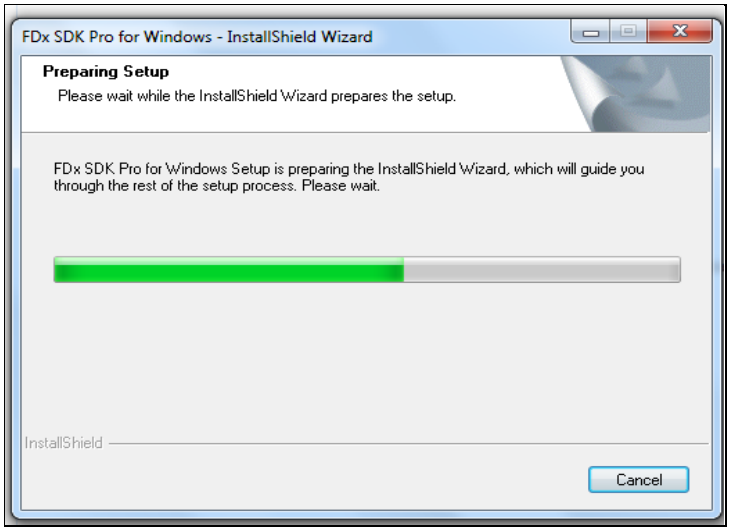


Figura 39. Inicio de Asistente de Instalación

Aceptar los términos de licencia, presionando la opción **Yes,** y continuar con la instalación

Finalmente aparecerá el mensaje que la instalación ha concluido y se presiona **Finish.**

Anexo 3.2: FDx SDK Pro for Java v1.4 rev593

Adicionalmente al FDx SDK Pro for Windows v3.7_J14, se requiere copiar los archivos de la carpeta FDx SDK Pro for Java v1.4 rev593 a las siguientes rutas dependiendo de la arquitectura del sistema operativo.

Windows 32bits: *jnifplib\win32\jnisgfplib.dll a la ruta: C:\windows\system32*

Windows 64bits: *jnifplib\win32\jnisgfplib.dll a la ruta C:\Windows\SysWOW64*

jnifplib\x64\jnisgfplib.dll a la ruta C:\Windows\system32

Anexo 3.3: Instalación y Configuración de Driver SecuFMASetup para el dispositivo SecuGenHamster PRO 20.

La instalación y configuración el driver del dispositivo SecuGenHamster PRO 20 se realizará de la siguiente manera. Ejecutar el instalador del driver del dispositivo, con el lector conectado.

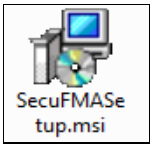


Figura 40. Setup Driver SecuGenHamster PRO 20.

Al seleccionarse el ejecutable, empieza con la copia de las librerías de control en el Sistema como se observa en la Figura 41, debemos seleccionar un dedo con el cual presionamos el dispositivo repetitivamente hasta finalizar la instalación correcta.

Figura 41. Instalación del driver SecuGen.

Anexo 4: Certificado de Traducción de Resumen

Washington ENGLISH INSTITUTE

WEIL - Nº 0000165

Más práctica por minuto... menor tiempo de aprendizaje.....

Yo, Freddy Castillo Hoyos, profesor del Instituto Washington;

Certifico:

Que tengo el conocimiento y dominio de los idiomas español e inglés y que las traducciones de los siguientes:

RESUMEN del tema:

"Disminución de la Suplantación de Identidad dentro de una Plataforma Virtual de Aprendizaje mediante la Autenticación por Huella Dactilar"

para: BRAVO BRITO DARÍO IGNACIO
TROYA IRIARTE MARÍA MAGDALENA

es verdadero y correcto a mi mejor saber y entender.

Firmado en Loja a los veintinueve días del mes de abril de 2015.

WASHINGTON ENGLISH
Formar Cia Ltda
DIRECCION ACADEMICA
Loja - Ecuador

24 de Mayo 11 - 20 y Azuay - 2573489 - 2579934

Anexo 5: Licencia Creative Commons

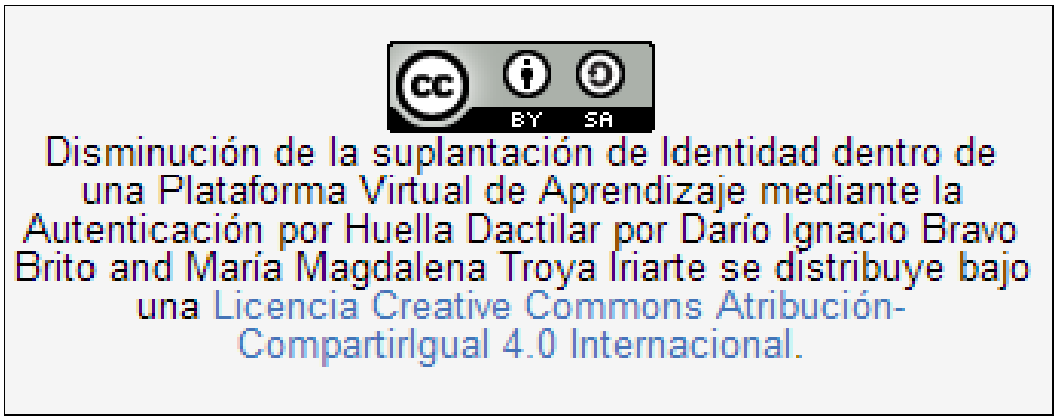


Figura 42. Licencia Creative Commons