eib01035896810

Desarrollo de la interfaz de autenticación biométrica para el módulo de préstamos del Sistema de Bibliotecas Koha de la Escuela Politécnica Nacional (Ecuador)

María José Bravo Ramos*
María Fernanda Portilla Pedraza**

Artículo recibido:
17 de septiembre de 2024
Artículo aceptado:
18 de febrero de 2025

Artículo de investigación

Resumen

Se desarrolló una interfaz de autenticación biométrica para el sistema de gestión de bibliotecas Koha en la Escuela Politécnica Nacional con el objetivo de mejorar la seguridad en la identificación de usuarios y reducir el acceso no autorizado. Se utilizó la metodología Scrum, que promueve un enfoque ágil y colaborativo. La interfaz fue diseñada para operar con un lector de huellas dactilares SecuGen, que integró las tecnologías necesarias y se adaptó a los requisitos del sistema Koha, el cual está desarrollado con el lenguaje de programación Perl. La implementación de la interfaz logró establecer una comunicación efectiva entre el sistema biométrico y Koha

* Biblioteca General, Escuela Politécnica Nacional, Ecuador
maria.bravor@epn.edu.ec
** Departamento de Seguridad de la Información, Universidad de las Américas, Ecuador
maria.portilla@udla.edu.ec

y superó los desafíos técnicos derivados de las diferencias entre los lenguajes de programación. Además, se comprobó que el sistema centralizado de bibliotecas facilita el mantenimiento y garantiza la protección de la información. El uso de esta interfaz contribuye a reducir el fraude de identidad y la pérdida de material bibliográfico; también subraya la necesidad de fortalecer la seguridad de la información en las bibliotecas ajustándose a lo estipulado en la Ley Orgánica de Protección de Datos Personales de Ecuador. La metodología de desarrollo empleada fue la más adecuada, pues aseguró avances eficientes para la biblioteca y cumplió con las expectativas de los usuarios del sistema.

Palabras clave: Bibliotecas universitarias; Desarrollo de software; Seguridad de la información; Software de bibliotecas

Development of a Biometric Authentication Interface for the Koha's Library System Loan Module at the National Polytechnic School (Ecuador)

María José Bravo Ramos and *María Fernanda Portilla Pedraza*

Abstract

To enhance user identification security and reduce unauthorized access, we developed a biometric authentication interface for the Koha Library management system at the National Polytechnic School. The project employed the Scrum methodology, which promotes an agile and collaborative approach. The interface was designed to operate with a SecuGen fingerprint reader that integrated the necessary technologies and adapted to the requirements of the Koha system, which was developed with the programming language Perl. The interface implementation successfully established effective communication between the biometric system and Koha and overcame technical challenges that may have arisen due to programming language differences. Furthermore, we confirmed that the centralized library system facilitates its maintenance and ensures information protection. Usage of this interface not only helps to reduce identity fraud and library material loss but underscores the need to strengthen information security in libraries in accordance with the Organic Law on Personal Data Protection [Ley Orgánica de

Protección de Datos Personales] of Ecuador. The development methodology used proved to be the most suitable since it ensured efficient progress for the library and met the expectations of the system's users.

Keywords: University Libraries; Software Development; Information Security; Library Software

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Introducción

La seguridad de la información se ha convertido en una necesidad imperiosa para todas las organizaciones debido a la constante evolución de la tecnología, especialmente en lo que respecta a los datos personales. En un entorno donde la información es el activo más valioso, esencial para tomar decisiones acertadas y desarrollar estrategias de negocio, es fundamental considerar las vulnerabilidades existentes y los riesgos asociados a los ciberataques. Es común escuchar sobre incidentes de espionaje o robo de información a empresas y entidades financieras, lo que resalta la necesidad de implementar medidas de seguridad basadas en protocolos que garanticen la confidencialidad, integridad y disponibilidad de los datos (Sierra Ramos, 2012: 69).

Las bibliotecas, que gestionan datos sensibles sobre sus usuarios, como datos personales, multas e información bibliográfica, poseen datos cruciales para el funcionamiento de la organización. Sin embargo, a pesar de la importancia de esta información, muchas bibliotecas aún no han implementado protocolos de seguridad adecuados, en parte debido a que sus administradores no comprenden su relevancia. Un ejemplo de implementación exitosa es el caso de la biblioteca de la Universidad Shih Hsin, ubicada en Taipéi, que integró tecnología de cadenas de bloques (*blockchain*) y biometría dactilar en su sistema de préstamos (Fu, 2020).

La tecnología de cadenas de bloques es definida como un sistema de registros de datos inmutables, y con fecha de caducidad, gestionado por una red descentralizada de servidores que no pertenecen a ninguna entidad individual. En este sistema, cada bloque de datos está asegurado y vinculado con los demás mediante principios criptográficos, sin necesidad de una autoridad central. Esta estructura habilita la distribución segura y cifrada de la información, garantizando que las transacciones no puedan ser alteradas por usuarios no autorizados.

Por otro lado, la biometría ha emergido como una solución automatizada y precisa para el reconocimiento de personas, basándose en características físicas o conductuales únicas, como huellas dactilares, iris, voz, rostro, escritura

y geometría de la mano (Interpol, s. f.; Sánchez Gómez, 2020). Este enfoque ofrece una autenticación robusta, pues los datos biométricos son inherentemente únicos y difíciles de falsificar, lo cual los convierte en una opción ideal para proteger sistemas críticos y garantizar la identidad de los usuarios. Su implementación ha aumentado significativamente en aplicaciones como el control de acceso y la seguridad en dispositivos electrónicos.

Entre las características biométricas más utilizadas están las huellas dactilares, el reconocimiento facial, el análisis del iris y la voz (Grupo Arga, s. f.), cada una con sus propias ventajas y desafíos en términos de precisión, facilidad de uso y seguridad. Las huellas dactilares constituyen uno de los métodos de autenticación biométrica más utilizados debido a su rapidez, facilidad de obtención, alto nivel de precisión y excelente relación costo-beneficio. Además, ofrecen comodidad y fiabilidad en la lectura de los datos. Esta técnica de verificación biométrica se considera menos intrusiva y ha sido utilizada durante mucho tiempo, pues ha demostrado ser altamente confiable ya que no existen dos huellas dactilares idénticas (Ferreira, 2023).

En el ámbito internacional, los datos biométricos, como las huellas dactilares, son considerados como datos sensibles debido a su capacidad para identificar a un individuo de manera única. Esto implica que su manejo debe regirse por estrictas normativas y estándares éticos que aseguren la protección de la privacidad de los usuarios. En este sentido, es crucial que los sistemas que emplean biometría para la autenticación, como el proyecto propuesto de autenticación mediante huellas dactilares, cumplan con los marcos legales establecidos (Lumini, Nanni y Maltoni, 2009: 340).

El creciente uso de la biometría plantea, sin embargo, inquietudes sobre la privacidad y la protección de los datos. Por ello, resulta esencial instaurar medidas de seguridad adecuadas para mitigar los riesgos asociados y garantizar un manejo responsable de los datos personales y sensibles, incluidos los biométricos. En Ecuador, hasta el momento no se ha localizado algún estudio o bibliografía relacionada con la implementación de biometría en los procesos de préstamo e material bibliográfico en las bibliotecas del país.

La Escuela Politécnica Nacional (en adelante, EPN) ha utilizado el paquete informático Koha para realizar la gestión de las bibliotecas desde el año 2014, el cual posee los módulos de catalogación, búsqueda avanzada, administración, circulación, usuarios, autoridades, informes, herramientas, preservación, entre otros (Koha Community, 2025). El módulo de usuarios del sistema Koha solamente permite identificar al solicitante, pero en ningún momento lo autentica biométricamente; esto implica que el usuario podría solicitar préstamos y entregar un documento vigente aunque no sea de su pertenencia sin que Koha verifique que la persona es quien dice ser. Además, no se ha implementado un

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

mecanismo adecuado de resguardo de los datos sensibles de los usuarios. Las últimas actualizaciones del Sistema de Bibliotecas tampoco han integrado soluciones biométricas, lo que aumenta el riesgo de que usuarios no autorizados puedan acceder a la información, con las consecuencias negativas que ello podría implicar.

En este contexto, la Ley Orgánica de Protección de Datos Personales, promulgada en 2021, establece un marco legal que obliga a las entidades públicas y privadas a gestionar los datos de forma responsable, garantizando que los ciudadanos mantengan el control sobre su información personal. Entre los principios clave de esta ley, destacan la transparencia, el consentimiento informado y la seguridad, exigiendo que los responsables del tratamiento obtengan el consentimiento explícito del titular para procesar sus datos personales y, especialmente, sus datos sensibles, especificando los fines para los cuales se utilizarán y las medidas de seguridad implementadas para protegerlos.

Con base en lo anterior, la implementación de tecnologías biométricas para la autenticación de usuarios en el módulo de préstamos del sistema bibliotecario de la EPN surge como una solución eficaz para reducir el fraude de identidad. No obstante, debido a la naturaleza sensible de los datos biométricos es esencial que, además de integrar la interfaz de autenticación biométrica a Koha, su tratamiento cumpla con la legislación ecuatoriana de protección de datos. Esto implica que los datos, como las huellas dactilares, deben recolectarse y almacenarse con el consentimiento explícito del usuario, asegurando su protección adecuada para evitar cualquier uso indebido.

Con estos antecedentes, y a partir del estudio ya realizado en Bravo Ramos y Portilla Pedraza (2015), el objetivo principal de este proyecto es desarrollar una interfaz de autenticación biométrica e integrarla al módulo de circulación y préstamo del Sistema de Bibliotecas Koha de la EPN, utilizando la lectura de huellas dactilares como método de autenticación de usuarios

Metodología

Para cumplir con el desarrollo de la interfaz de autenticación biométrica del módulo de préstamos, se aplicó la metodología investigación-acción (*action research)*, la cual define tres pasos clave que se adaptan fácilmente al desarrollo del proyecto. En primer lugar, se realizó un diagnóstico del problema actual que enfrentan las bibliotecas de la EPN en relación con la seguridad de la información de sus usuarios durante el proceso de préstamo. Este diagnóstico es fundamental como punto de partida para la implementación de una solución adecuada a fin de evitar el fraude de identidad de los usuarios de la biblioteca.

A continuación, se inició la fase de acción, que implicó la ejecución de cambios en la biblioteca para abordar el problema identificado. Durante esta fase, se recopiló información sobre soluciones tecnológicas que pudieran prevenir el fraude de identidad, enfocándose en aspectos como la seguridad de la información, facilidad de uso y compatibilidad con el sistema Koha. Entre las opciones investigadas, destacó el uso de la biometría mediante la lectura de huellas dactilares. Al observar que Koha no implementaba esta solución, se decidió desarrollar una interfaz de autenticación biométrica que se le integrara. Este proceso requirió la investigación de metodologías de desarrollo de *software* apropiadas para el proyecto. En este contexto, se identificaron dos grupos principales de metodologías de desarrollo: tradicionales y ágiles.

Las metodologías tradicionales se centran, principalmente, en la generación de abundante documentación a lo largo del proyecto, lo que implica altos costos para implementar cambios. Además, estas metodologías no se adaptan bien a los nuevos requisitos de los usuarios y son menos efectivas en entornos cambiantes.

Entretanto, las metodologías ágiles priorizan la satisfacción del cliente y su participación activa durante todo el proceso de desarrollo, lo que permite una adaptación rápida a los cambios y la entrega de productos en plazos más cortos, que ahorra tiempo y costos. Estas metodologías también promueven entregas parciales del producto y utilizan equipos pequeños que generan poca documentación.

Para la selección de la metodología ágil se procederá a realizar un análisis comparativo entre las más utilizadas: Scrum y XP. Scrum, debido a su enfoque en la gestión ágil de proyectos y la colaboración continua entre los miembros del equipo, facilita una rápida adaptación a los cambios y asegura de que se cumplan los requisitos del proyecto mediante ciclos cortos de desarrollo llamados *sprints*, basados en las historias de usuario (Martins, 2025). Por su parte, la programación extrema (XP) se enfoca en prácticas de programación, como la programación en pareja y el desarrollo iterativo también dividido en sprints. Sin embargo, XP es más disciplinada que Scrum, ya que impone reglas y pautas estrictas para promover la interacción constante entre desarrolladores y clientes (Raeburn, 2025).

A continuación, la *Tabla 1* presenta una comparativa entre las características del proyecto y las metodologías Scrum y XP, donde se valoran los puntos de cumplimiento de cada una. Para la valoración de cada característica, se usarán valores de cumplimiento entre 1 (no cumplimiento) y 5 (cumplimiento óptimo):

Características del proyecto	Scrum	XP
Poco número de iteraciones	5	4
Entrega en corto tiempo	5	5
Personal limitado	5	3

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Integración del equipo de programación con el cliente	5	5
Desarrollo iterativo	5	5
Total	**25**	**22**

Tabla 1. Matriz comparativa XP - Scrum
Fuente: elaboración de las autoras (2024)

Según los valores obtenidos, la metodología ágil más adecuada para este proyecto es Scrum, debido a la necesidad de coordinar el trabajo entre varios equipos, como el encargado del desarrollo de la interfaz biométrica y el equipo responsable de la integración con Koha. Tras definir la metodología de desarrollo, y conforme con las fases establecidas en la misma, se gestionaron los aspectos necesarios para llevar a cabo la recopilación de requisitos de los usuarios de la biblioteca; se revisaron los requerimientos técnicos para el diseño y desarrollo de la interfaz, así como la realización de las pruebas unitarias y del sistema con el fin de verificar que la aplicación cumple con los requisitos establecidos para las bibliotecas de la EPN.

Finalmente, se evaluó tanto el funcionamiento de la interfaz como el nivel de satisfacción del equipo de la biblioteca, con el objetivo de garantizar el cumplimiento de los objetivos del proyecto. En primer lugar, se proporcionó acceso al software a los bibliotecarios para que probaran su funcionalidad. Posteriormente, se recopiló y analizó la retroalimentación sobre el rendimiento y la aceptación de la interfaz de autenticación biométrica mediante una encuesta elaborada en Google Forms. Esta encuesta constaba de seis preguntas de tipo ordinal y su enlace de acceso fue enviada por correo electrónico a los ocho usuarios del Sistema de Bibliotecas, quienes son los bibliotecarios responsables de cada una de las bibliotecas satélite.

Desarrollo de la interfaz de autenticación biométrica

Requisitos

Si comparamos las necesidades de las bibliotecas de la EPN de hace unos años con las actuales, resalta que es ineludible utilizar las tecnologías de la información y la comunicación para su adecuada administración, lo que favorece la productividad y facilita la toma de decisiones. Un elemento importante para tomar en cuenta es el uso de herramientas de software libre, ya que el costo del desarrollo de los sistemas es menor.

Actualmente el software que gestiona las bibliotecas es Koha, en su versión estable 23.11, totalmente libre. Este sistema funciona con una arquitectura

cliente-servidor; utiliza GNU/Linux, Apache, MariaDB, Perl, phpMyAdmin y OpenLDAP en el servidor y cualquier navegador web por parte del cliente. Koha es compatible con los lenguajes de programación Java y PHP (Koha Community, 2025), lo cual permite su integración con desarrollos realizados bajo las referidas plataformas a través de servicios web. Por esta razón, para el desarrollo de la interfaz de autenticación biométrica para el módulo de préstamos se utilizará Java.

Además, la biblioteca estándar de Java la componen varias librerías que facilitan la operación en el lenguaje y dispositivos externos. Para tomar las huellas dactilares se usará el dispositivo biométrico Hamster Plus de SecuGen Corporation, acompañado de la librería SecuSearch SDK (*Figura 1*).

Figura 1. Lector de huellas dactilares
Fuente: SecuGen (s. f.)

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Este lector es totalmente compatible con el entorno de desarrollo Java y utiliza sensores ópticos para obtener una imagen de la huella dactilar; durante su funcionamiento, este dispositivo toma dos muestras y, antes de comparar la muestra obtenida con una almacenada previamente, el software comprueba que la muestra tomada sea válida y hace los ajustes necesarios en caso de requerir una nueva toma (Salcedo Polanco, Sempértegui Jácome e Hidalgo Lascano, 2010: 1).

Para comparar huellas dactilares deben ubicarse los puntos de minucia, los cuales son zonas donde terminan o se bifurcan las crestas papilares, y se miden las posiciones que tienen; una forma de hacerlo es trazando líneas rectas sobre ellos, con lo cual puede obtenerse una figura única para cada dedo (Sadurní, 2021; Tan, Bhanu y Wang, 2009: 370).

Por otro lado, para desarrollar la interfaz de autenticación de acuerdo con la metodología Scrum debe partirse desde la recopilación de sus requisitos (Urteaga Pecharromán, 2015). Esto se determina por medio de las historias de usuario. Adicionalmente, los roles resultaron asignados de la siguiente manera (Caroli, 2023):

- Dueño del producto: Responsable de bibliotecas
- Scrum Master: Director del proyecto
- Equipo de desarrollo: Asistentes de las TIC

Las historias de usuario han sido identificadas por medio de entrevistas al dueño del producto, la *Tabla 2* describe el requerimiento de captura de las huellas dactilares:

Historia del usuario	
Número: 1	**Usuario:** Responsable de bibliotecas
Nombre: Capturar huellas dactilares	
Prioridad en el negocio: alta	**Riesgo en desarrollo:** bajo
Puntos estimados: 3	**Iteración asignada:** 1
Programadores responsables: Asistentes de las TIC	
Descripción: quiero que tome máximo dos muestras de la huella dactilar del dedo índice del usuario.	
Validación: el referencista podrá visualizar las imágenes capturadas de la huella dactilar.	

Tabla 2. Historia de usuario "Capturar huellas dactilares"
Fuente: elaboración de las autoras (2024)

Las historias de usuario identificadas para el resto de los requerimientos están en el *Anexo A*.

Siguiendo con la metodología de desarrollo, en función de los requerimientos recopilados, la *Tabla 3* detalla el conjunto de tareas (*product backlog*) que darán funcionalidad a la interfaz de autenticación biométrica para cumplir con los requerimientos del sistema. Esta tabla incluye la complejidad de cada tarea; asigna un valor de 1 a la baja complejidad y 5 a la alta complejidad, así como las prioridades de las tareas definidas por el cliente, donde 1 representa a la prioridad más urgente y 5 a la menos urgente.

Nro.	Tareas	Complejidad	Prioridad
1	Diseño del modelo de base de datos	3	4
4	Diseño de la interfaz	3	4
5	Instalación del entorno de desarrollo	5	5
6	Generación del código para el funcionamiento de la interfaz de autenticación biométrica	4	5
7	Conexión de la interfaz de autenticación con el motor de la base de datos	4	4
8	Modificación de código en la interfaz de préstamo de Koha	3	5
9	Implementación de la interfaz de autenticación biométrica	3	5
10	Pruebas de unidad	3	5
11	Integración de la interfaz de autenticación biométrica con el módulo de préstamos del Sistema de Bibliotecas	5	5
12	Pruebas de sistema	3	5

Tabla 3. Tareas por realizar (product backlog)
Fuente: elaboración de las autoras (2024)

Posteriormente, las tareas descritas se distribuirán en cuatro sprints, en Scrum es una forma de subdividir el proyecto para conseguir realizarlo de forma más eficiente y ágil (Urteaga Pecharromán, 2015). A continuación, se presenta el *sprint backlog*, es decir, la lista de tareas que el equipo Scrum finalizará durante el primer sprint en la *Tabla 4*; la planificación está prevista para una duración de 6 días. Los sprints restantes pueden consultarse en el *Anexo B*.

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Nro.	Tarea	Responsables	Tiempo estimado (días)
1	Diseño del modelo de la base de datos	Asistentes de las TIC	3
4	Diseño de la interfaz	Asistentes de las TIC	3
		Total	6

Tabla 4. Tareas del primer sprint
Fuente: elaboración de las autoras (2024)

Diseño

Para cumplir las tareas estipuladas en el primer sprint, se procedió con el diseño del modelo físico de la base de datos según los requerimientos de la interfaz de autenticación biométrica. La base de datos utilizada para el desarrollo de la interfaz se llama HuellaBase y contiene una única entidad llamada 'huella', como indica la *Figura 2*.

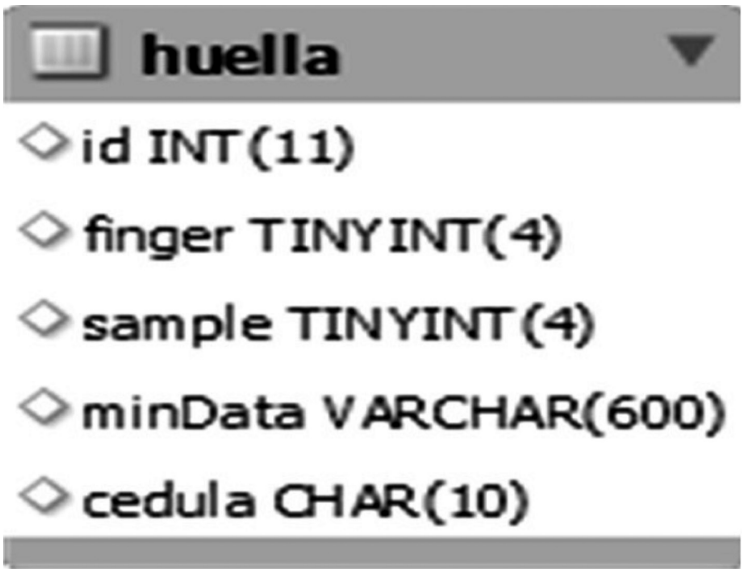

Figura 2. Entidad 'huella'
Fuente: captura del motor de base de datos MariaDB (2024)

Posteriormente, la *Figura 3* indica el diseño de la interfaz de autenticación biométrica para la captura y el registro de huellas dactilares de los usuarios de las bibliotecas de la EPN, la cual se diagramó con Pencil, herramienta de diseño de interfaces gratuita y de código abierto.

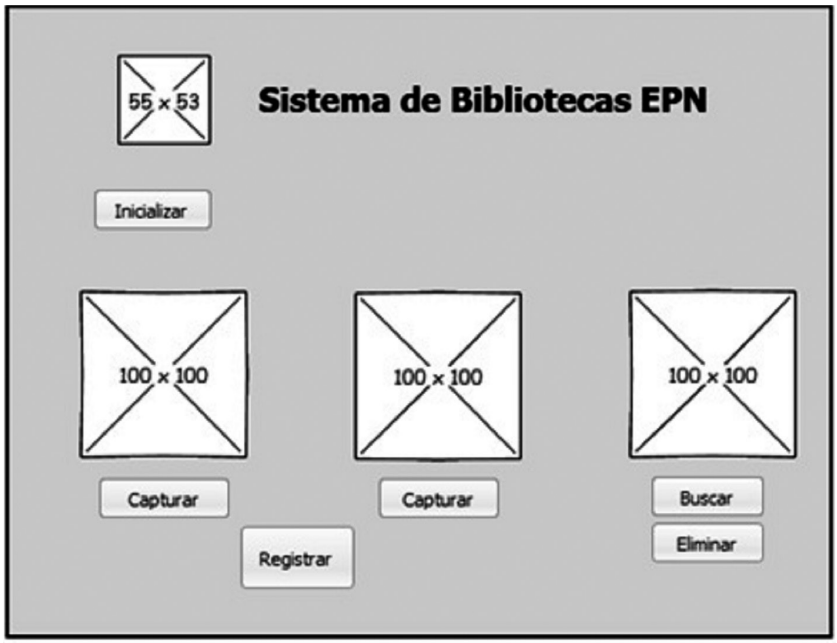

Figura 3. Diseño de la interfaz de autenticación biométrica
Fuente: captura de Pencil (2024)

Durante el segundo sprint sucedió la instalación del entorno de desarrollo para la interfaz de autenticación biométrica y el Sistema de Bibliotecas Koha. Además, se generó el código de la interfaz mediante la clase HuellaInterfaz.java y que se conectó con la base de datos HuellaBase.

Implementación

Esta tarea sucedió en el tercer sprint y habilitó la puesta en marcha de la interfaz de autenticación biométrica. Para el correcto funcionamiento de la interfaz se implementó un servicio web SOAP desarrollado en el entorno Microsoft Visual Studio. La integración entre el servicio web SOAP y la interfaz desarrollada en el entorno Java se efectuó por medio de la librería SecuSearch SDK Pro, proveído por la empresa SecuGen. La *Figura 4* presenta la interfaz de autenticación biométrica con sus seis opciones:

- La opción Inicializar comienza al lector de huellas dactilares.
- La opción Capturar izquierda toma la primera muestra de la huella dactilar del usuario a través del lector y la mostrará en el área de imagen superior izquierda.

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

- La opción Capturar derecha toma la segunda muestra de la huella dactilar del usuario a través del lector y la mostrará en el área de imagen superior derecha.
- La opción Registrar almacena las dos muestras de la huella dactilar en la base de datos asociadas a la cédula de identidad del usuario. Las huellas dactilares son almacenadas y transmitidas a través del cifrado AES de 256 bits, un estándar reconocido para garantizar la seguridad de los datos.
- La opción Buscar captura la huella dactilar y realiza su búsqueda en la base de datos y retornará como resultado el número de cédula del usuario.
- La opción Eliminar busca la huella dactilar del usuario y la suprime de la base de datos.

Figura 4. Interfaz de autenticación biométrica
Fuente: captura tomada desde Java (2024)

Ejecución de pruebas

Estas pruebas permiten comprobar el correcto funcionamiento del código de la interfaz de autenticación biométrica y se desarrollarán a partir de los requisitos de esta. Cada caso de prueba se realizó en función de las historias de usuario identificadas. La *Tabla 5* muestra el caso de prueba para el requerimiento de la captura de huellas dactilares.

Prueba de unidad	
Número de caso de prueba: 1	**Número de historia de usuario:** 1
Nombre de caso de prueba: Capturar huellas dactilares	
Descripción: se capturan dos veces las huellas dactilares del dedo índice derecho del usuario. **Pasos de ejecución:** 1. Se muestra la pantalla principal de la interfaz. 2. El usuario coloca su dedo índice sobre el lector de huellas dactilares. 3. Se presiona el botón Capturar izquierda. 4. Se visualiza la primera muestra de la huella dactilar. 5. El usuario coloca su dedo índice sobre el lector de huellas dactilares por segunda ocasión. 6. Se presiona el botón Capturar derecha. 7. Se visualiza la segunda muestra de la huella dactilar.	
Resultado esperado: la aplicación presenta las dos muestras de la huella dactilar capturadas por el dispositivo biométrico.	**Resultado obtenido:** la aplicación ha capturado correctamente las dos muestras de la huella dactilar a través del dispositivo biométrico.
Acciones correctivas: ninguna	
Evaluación: correcta	

Tabla 5. Caso de prueba "Capturar huellas dactilares"
Fuente: elaboración de las autoras (2024)

Los casos de pruebas efectuados para el resto de los requerimientos pueden consultarse en el *Anexo C*.

Integración de la interfaz con el módulo de préstamos

Esta tarea pertenece al cuarto sprint que es parte de la planificación de sprints. En este se integra la interfaz de autenticación biométrica con el módulo de préstamos del Sistema de Bibliotecas. Y debido a que la arquitectura del sistema Koha es de tipo cliente-servidor, fue necesario formar una red con dos equipos con sus respectivas configuraciones para establecer conectividad.

Para integrar la interfaz de autenticación biométrica al módulo de préstamos de Koha deben realizarse las configuraciones en el archivo "jquery.js", ubicado en el directorio "/usr/share/koha/intranet/htdocs/intranet-tmpl/lib/jquery/jquery.js" del servidor. Este archivo contiene el código fuente de la página principal del Sistema de Bibliotecas Koha. Por otro lado, en la aplicación de autenticación biométrica, se agrega el enlace del servidor que contiene el puerto de comunicación y la variable de la cédula de identidad del usuario que registró su huella dactilar codificada en lenguaje java. Todo este código está incluido dentro del botón Buscar.

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Para este proyecto, debido a la complejidad y funcionalidad brindada por el software, estas pruebas se realizaron a la par de las del sistema. El propósito de estas es comprobar que se haya integrado adecuadamente el módulo de préstamos del Sistema de Bibliotecas con la interfaz de autenticación biométrica y que realizan las funciones esperadas.

Para verificar la interacción de los componentes, se realizaron las pruebas del sistema. La *Tabla 6* muestra el caso de prueba para el requerimiento de captura de huellas dactilares.

Caso de prueba
Número de caso de prueba: 1
Nombre de caso de prueba: Capturar huellas dactilares
Descripción: se capturan dos veces las huellas dactilares del dedo índice derecho del usuario. **Pasos de ejecución:** 1. Se registran los datos del usuario en Koha. 2. Se visualiza la pantalla principal de la interfaz. 3. El usuario coloca su dedo índice sobre el lector de huellas dactilares. 4. Se presiona el botón Capturar izquierda. 5. Se visualiza la primera muestra de la huella dactilar. 6. El usuario coloca su dedo índice sobre el lector de huellas dactilares por segunda ocasión. 7. Se presiona el botón Capturar derecha. 8. Se visualiza la segunda muestra de la huella dactilar.
Resultado esperado: el sistema presenta las dos muestras de la huella dactilar capturadas por el dispositivo biométrico.
Resultado obtenido: el sistema ha capturado correctamente las dos muestras de la huella dactilar a través del dispositivo biométrico.
Evaluación: correcta

Tabla 6. Caso de prueba "Capturar huellas dactilares"
Fuente: elaboración de las autoras (2024)

Los casos de pruebas de sistemas para el resto de los requerimientos están descritos en el *Anexo D*.

Resultados

El sistema integrado de bibliotecas, conformado por Koha y la interfaz de autenticación biométrica, funciona de la siguiente manera:

1. Ingreso al módulo de usuarios y registro de un usuario del sistema integrado en Koha. La *Figura 5* y *Figura 6* muestran la creación de un nuevo usuario; para este proyecto es importante contar con su cédula de identidad. Además, para asegurar la protección de los datos personales, es necesario obtener la firma del usuario mediante una forma de consentimiento informado que autorice el uso exclusivo de sus datos biométricos para el proceso de préstamo de material bibliográfico, cumpliendo así con la Ley de Protección de Datos Personales de Ecuador.

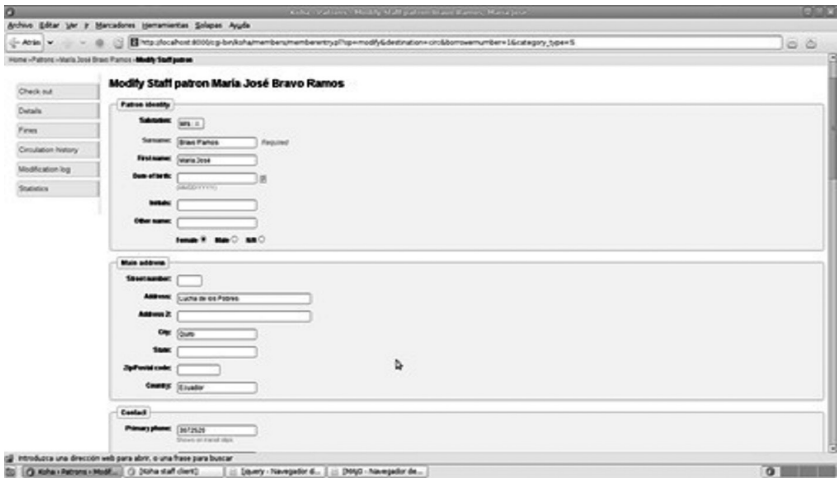

Figura 5. Creación de usuario en Koha
Fuente: captura tomada desde Koha (2024)

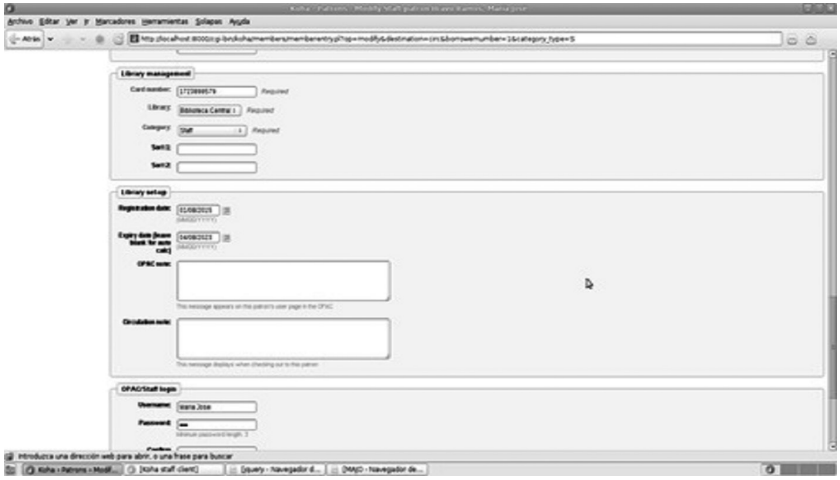

Figura 6. Creación de usuario en Koha
Fuente: captura tomada desde Koha (2024)

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

2. En la interfaz de autenticación biométrica, seleccionar la opción Inicializar para habilitar el dispositivo biométrico y sus opciones (*Figura 7*).

Figura 7. Interfaz de autenticación biométrica
Fuente: captura tomada desde Java (2024)

3. A continuación, debe tomarse la huella dactilar del usuario, quien debe colocar su dedo sobre el lector de huellas. Al presionar el botón Capturar izquierda puede observarse la primera muestra de la huella dactilar (*Figura 8*).

Figura 8. Primera muestra de huella dactilar
Fuente: captura tomada desde Java (2024)

4. Luego, debe tomarse la segunda muestra de la huella presionando el botón Capturar derecha (*Figura 9*).

Figura 9. Segunda muestra de huella dactilar
Fuente: captura tomada desde Java (2024)

5. Después, procede a almacenarse la huella dactilar en la base de datos de la interfaz. Al presionar el botón Registrar, aparece un cuadro de diálogo solicitando el ingreso de la cédula de identidad del usuario asociada a las huellas dactilares capturadas en el paso anterior (*Figura 10*). El número de cédula de identidad debe ser el mismo registrado al momento de crear el usuario en Koha en el paso 1.

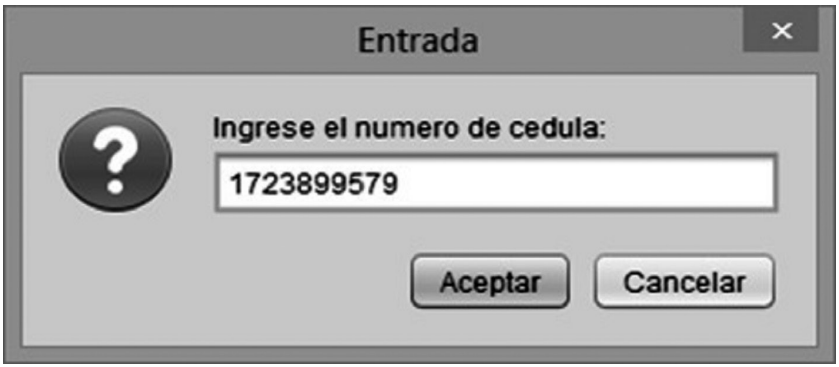

Figura 10. Ingreso del número de cédula del usuario registrado en Koha
Fuente: captura tomada desde Java (2024)

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

6. Finalmente, se muestra un mensaje de confirmación de registro exitoso (*Figura 11*). Internamente, la información de las huellas dactilares resulta almacenada con cifrado asimétrico AES de 256 bits.

Figura 11. Confirmación de registro exitoso
Fuente: captura tomada desde Java (2024)

A continuación, se describe el proceso de búsqueda de huella dactilar de la interfaz de autenticación biométrica y su integración con Koha:

1. Procede a tomarse la huella dactilar del usuario registrado, quien debe colocar su dedo sobre el lector de huellas. Al presionar el botón Buscar, puede observarse la huella dactilar (*Figura 12*).

Figura 12. Interfaz de autenticación biométrica
Fuente: captura tomada desde Java (2024)

2. Si la huella dactilar del usuario fue registrada anteriormente, debe accederse a la página de préstamos del sistema integrado de bibliotecas Koha y enviar como parámetro en el URL el número de cédula que se busca (*Figura 13*).

Figura 13. Página principal de Koha
Fuente: captura tomada desde Koha (2024)

3. La *Figura 14* muestra la búsqueda del usuario a través de su número de cédula y el préstamo al usuario encontrado.

Figura 14. Interfaz de préstamo de Koha
Fuente: captura tomada desde Koha (2024)

De esta manera, la interfaz de autenticación biométrica interactúa con el módulo de préstamos del Sistema de Bibliotecas Koha, como si se tratara de un solo sistema.

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Posteriormente, el equipo de bibliotecarios fue incorporado para evaluar el funcionamiento de la interfaz. A tal fin, obtuvieron acceso al aplicativo y se les solicitó completar una encuesta con el objetivo de analizar los resultados y medir su nivel de aceptación. La encuesta fue respondida por los ocho bibliotecarios, usuarios del sistema, la cual alcanzó una tasa de respuesta de 100 %. Los resultados obtenidos en cada una de las preguntas de la encuesta se presentan a continuación (*Figura 15* - *Figura 20*).

Se les consultó a los bibliotecarios si la interfaz de autenticación biométrica les ha ayudado a garantizar la identidad del usuario. La *Figura 15* muestra que 75 % de los bibliotecarios considera que esta ha sido eficaz para garantizar la identidad del usuario, lo que implica que ahora pueden realizar los préstamos de forma segura y confiable.

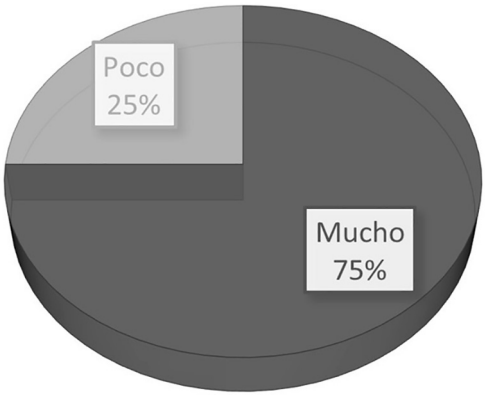

Figura 15. Aporte de la interfaz para garantizar la identidad del usuario
Fuente: elaboración de las autoras (2024)

En cuanto al grado de dificultad que los bibliotecarios encuentran al utilizar la interfaz de autenticación biométrica, la *Figura 16* revela que 63 % de los bibliotecarios consideran que esta es fácil de usar, lo cual sugiere que es intuitiva, amigable y accesible.

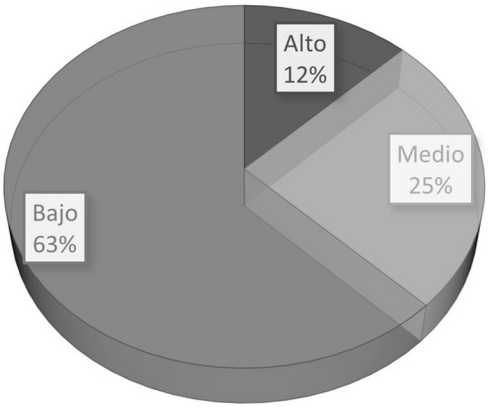

Figura 16. Dificultad durante el uso de la interfaz
Fuente: elaboración de las autoras (2024)

Respecto a la facilidad de captura y registro de las huellas dactilares a través de la interfaz, la *Figura 17* indica que 62 % de los bibliotecarios opina que las huellas dactilares se capturan y registran con facilidad, lo que refleja que la explicación de los requisitos fue adecuada.

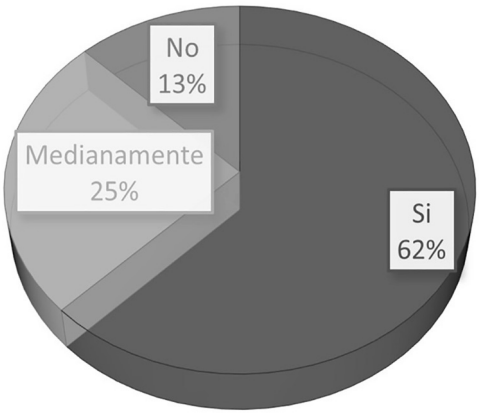

Figura 17. Captura y registro de las huellas dactilares
Fuente: elaboración de las autoras (2024)

En cuanto al tiempo de respuesta de la interfaz, la *Figura 18* muestra que 62 % de los bibliotecarios considera que el tiempo de respuesta es rápido, lo que indica que tiene un buen rendimiento.

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

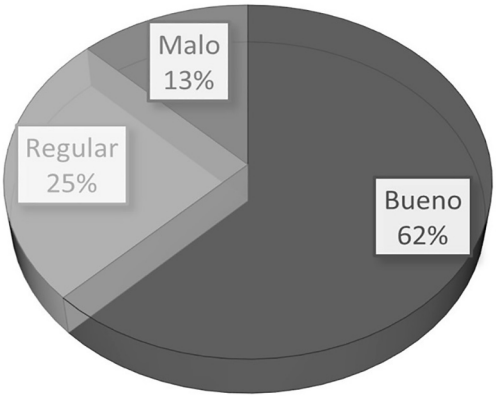

Figura 18. Tiempo de respuesta de la interfaz
Fuente: elaboración de las autoras (2024)

Sobre los colores y ubicación de los componentes en la interfaz de autenticación biométrica, la *Figura 19* expone que 75 % de los bibliotecarios está conforme con los colores y la disposición de sus elementos.

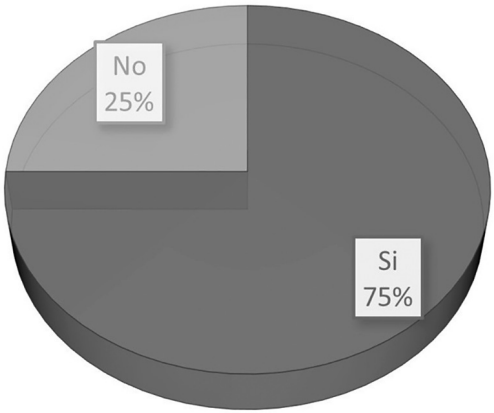

Figura 19. Colores y ubicación de los componentes de la interfaz
Fuente: elaboración de las autoras (2024)

En relación con la satisfacción de las necesidades de la biblioteca, la *Figura 20* muestra que 67 % de los bibliotecarios considera que la interfaz de autenticación biométrica satisface sus necesidades, lo que señala que la implementación fue exitosa.

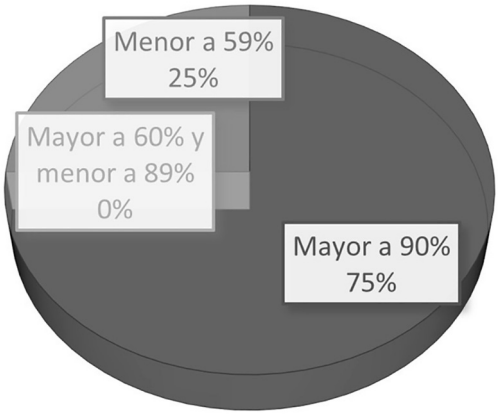

Figura 20. Satisfacción de las necesidades de la biblioteca
Fuente: elaboración de las autoras (2024)

A partir de los resultados obtenidos en la encuesta, la interfaz de autenticación biométrica:

- Cumple con la funcionalidad requerida por el dueño del producto, tal como se definió en la etapa de recopilación de requisitos.
- Es intuitiva y proporciona a los bibliotecarios una interfaz amigable durante la realización de cada proceso.
- Realiza las tareas de captura, registro, búsqueda y eliminación de huellas dactilares de forma rápida y segura.
- Garantiza su integración con Koha y el manejo adecuado del módulo de préstamos.

Conclusiones

El modelo de lector de huella dactilar SecuGen, utilizado en este proyecto, fue el más adecuado para el desarrollo del software porque se ajustó a las especificaciones establecidas por el dueño del producto.

Cuando se investigó la forma de actuar del Sistema de Bibliotecas de la Escuela Politécnica Nacional, pudo concluirse que es un sistema centralizado donde las bibliotecas existentes en la EPN, conocidas como bibliotecas satélite, se comunican directamente con la Biblioteca General, de donde extraen la información requerida. Esto implica ciertas ventajas, como la seguridad y la posibilidad de llevar a cabo un mantenimiento más fácil. Sin embargo, se espera que el rendimiento

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

y los tiempos de respuesta de Koha sean también adecuados, lo que hará que las consultas bibliográficas de los usuarios no demoren demasiado.

La implementación de la interfaz de autenticación biométrica ha demostrado ser efectiva para reducir el fraude de identidad de los usuarios, lo cual se traduce en una disminución sustancial de la pérdida de material bibliográfico por préstamos no autorizados. No obstante, es esencial que el sistema garantice la protección de los datos biométricos, especialmente dada la sensibilidad de esta información. La implementación de medidas, como el cifrado de datos, el consentimiento informado y el acceso controlado, contribuye a asegurar que los datos de los usuarios sean tratados con confidencialidad y en cumplimiento con la Ley Orgánica de Protección de Datos Personales de Ecuador.

La integración de la interfaz de autenticación biométrica con el sistema Koha resultó ser un desafío técnico debido a que Koha está desarrollado en Perl, mientras que la interfaz fue implementada en Java, un lenguaje elegido por su facilidad de transferencia de código. Esta diferencia de lenguajes generó dificultades de comunicación entre los sistemas. Para resolverlo, fue necesario revisar la documentación de Perl para entender el código fuente de Koha, identificar la estructura de su página principal y localizar el directorio donde se encontraba el archivo de configuraciones de Koha (jquery.js). A partir de ahí, se realizaron los ajustes pertinentes para integrar adecuadamente la interfaz de autenticación biométrica.

Considerando que el grado de aceptación de los usuarios encuestados fue alto, puede concluirse que la aplicación cumplió satisfactoriamente con las expectativas en cuanto a la facilidad de uso, el rendimiento, la eficiencia, la rapidez en el procesamiento de las tomas de las huellas dactilares y la seguridad de la información. En este sentido, se le recomienda al equipo de la biblioteca que la interfaz reciba mantenimiento a lo largo del tiempo, de tal manera que cuando la versión de Koha reciba actualizaciones, la interfaz de autenticación biométrica no pierda funcionalidad.

La metodología de desarrollo de la interfaz, Scrum, fue la más adecuada, puesto que permitió gestionar los diferentes componentes del proyecto de modo eficiente y asegurar que los requerimientos técnicos y funcionales planteados se cumplieran. El proyecto representa una mejora significativa en la gestión de los préstamos de material bibliográfico en la biblioteca de la EPN, y ofrece una base sólida para futuras mejoras en el sistema de autenticación y protección de datos biométricos de los usuarios institucionales.

Referencias

Apache Software Foundation. s. f. Apache HTTP Server Documentation. Consultado el 6 de agosto de 2024. https://httpd.apache.org/docs/

Bravo Ramos, María José, y María Fernanda Portilla Pedraza. 2015. "Desarrollo de la interfaz de autenticación biométrica para el módulo de préstamos del sistema de bibliotecas de la Escuela Politécnica Nacional". Tesis de grado, Escuela Politécnica Nacional. https://bibdigital.epn.edu.ec/handle/15000/10528

Caroli. 2023. "Scrum: Significado, aplicación, conceptos y ejemplos". Cultura Ágil, 4 de octubre. https://caroli.org/es/scrum-significado-aplicacion-conceptos-y-ejemplos/

Ferreira, Vinícius. 2023. "Basta el toque de un dedo para hacer frente a los desafíos de acceso y seguridad del mundo real". *Revista Seguridad 360*, 6 de noviembre. https://revistaseguridad360.com/noticias/seguridad-huellas-dactilares/

Fu, Meng-Hsuan. 2020. "Integrated Technologies of Blockchain and Biometrics Based on Wireless Sensor Network for Library Management". *Information Technologies and Libraries* 39 (3), e11883. https://doi.org/10.6017/ital.v39i3.11883

GNU Project. 2024. "GNU Development Resources". GNU Operating System. https://www.gnu.org/software/devel.en.html

Grupo Arga. s. f. "Huellas dactilares: guía completa para el análisis dactilar". Entradas. Consultado el 7 de mayo de 2024. https://argadetectives.com/huellas-dactilares-guia-completa-para-el-analisis-dactilar/

Interpol. s. f. "Huellas dactilares". Consultado el 13 de mayo de 2024. https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Huellas-dactilares

Koha Community. 2025. "Koha Manual (es)". https://koha-community.org/manual/latest/es/html/index.html

Lumini, Alessandra, Loris Nanni y Davide Maltoni. 2009. "Learning in Fingerprints". En *Biometrics: Theory, Methods and Applications*, editado por Nikolaos Boulgouris, Konstantinos Plataniotis y Evangelia Micheli-Tzanakou, 339-64. John Wiley and Sons. https://doi.org/10.1002/9780470522356.ch14

Martins, Julia. 2025. "Scrum: conceptos clave y cómo se aplica en la gestión de proyectos". Asana, 15 de febrero. https://asana.com/es/resources/what-is-scrum

Raeburn, Alicia. 2025. "La programación extrema (XP) produce resultados, pero ¿es la metodología adecuada para ti?". Asana, 13 de febrero. https://asana.com/es/resources/extreme-programming-xp

Sadurní, J. M. 2021. "La dactiloscopia, ciencia de las huellas dactilares". *National Geographic*, 25 de agosto. https://historia.nationalgeographic.com.es/a/dactiloscopia-ciencia-huellas-dactilares_17133

Salcedo Polanco, Juan Francisco, Paola Cecilia Sempértegui Jácome y Pablo William Hidalgo Lascano. 2010. "Desarrollo de una interfaz biométrica basada en la lectura de huellas dactilares para autenticación de usuarios en un cajero automático". En *Memorias de las XXIII Jornadas en Ingeniería Eléctrica y Electrónica (2010 J - FIEE)*. Quito: Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional. http://bibdigital.epn.edu.ec/handle/15000/3704

Sánchez Gómez, Jonny Julián. 2020. "Biometría y la seguridad informática en los métodos de autenticación". Tesis de especialización, Universidad Nacional Abierta y a Distancia, Colombia.
https://repository.unad.edu.co/handle/10596/39060

SecuGen. s. f. "Hamster Plus". Products. Consultado el 14 de agosto de 2024.
https://secugen.com/products/hamster-plus/

Sierra Ramos, Daniel. 2012. "Autenticación biométrica para comunicaciones inalámbricas a través de NFC". Tesis de grado, Universidad Carlos III de Madrid.
https://hdl.handle.net/10016/21258

Tan, Xuejun, Bir Bhanu y Rong Wang. 2009. "A Comparison of Classification and Indexing-Based Approaches for Fingerprint Identification". En *Biometrics: Theory, Methods and Applications*, editado por Nikolaos Boulgouris, Konstantinos Plataniotis y Evangelia Micheli-Tzanakou, 365-82. John Wiley and Sons.
https://doi.org/10.1002/9780470522356.ch15

Urteaga Pecharromán, Aitor. 2015. "Aplicación de la metodología de desarrollo ágil Scrum para el desarrollo de un sistema de gestión de empresas". Tesis de grado, Universidad Carlos III de Madrid.
https://hdl.handle.net/10016/23750

Para citar este texto:

Bravo Ramos, María José, y María Fernanda Portilla Pedraza. 2025. "'Desarrollo de la interfaz de autenticación biométrica para el módulo de préstamos del Sistema de Bibliotecas Koha de la Escuela Politécnica Nacional (Ecuador)". *Investigación Bibliotecológica: archivonomía, bibliotecología e información* 39 (103): 193-228.
http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Anexo A

Historia del usuario	
Número: 2	**Usuario:** Responsable de bibliotecas
Nombre de la historia: Registrar huella dactilar	
Prioridad en el negocio: alta	**Riesgo en desarrollo:** bajo
Puntos estimados: 3	**Iteración asignada:** 1
Programadores responsables: Asistentes de las TIC	
Descripción: quiero que la base de datos almacene las dos muestras de la huella dactilar capturadas asociadas al número de cédula del usuario.	
Validación: el referencista visualizará el mensaje de confirmación de que la huella dactilar se registró exitosamente, además verificará el registro de la huella dactilar del usuario a través de su búsqueda.	

Tabla 1. Historia de usuario "Registrar huella dactilar"
Fuente: elaboración de las autoras (2024)

Historia del usuario	
Número: 3	**Usuario:** Responsable de bibliotecas
Nombre de la historia: Buscar huella dactilar	
Prioridad en el negocio: alta	**Riesgo en desarrollo:** bajo
Puntos estimados: 3	**Iteración asignada:** 1
Programadores responsables: Asistentes de las TIC	
Descripción: quiero verificar que el usuario fue registrado correctamente en la base de datos mediante la lectura de su huella dactilar.	
Validación: el referencista visualizará el número de cédula del usuario en el área de búsqueda de la interfaz de préstamo del Sistema de Bibliotecas.	

Tabla 2. Historia de usuario "Buscar huella dactilar"
Fuente: elaboración de las autoras (2024)

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Historia del usuario	
Número: 4	**Usuario:** Responsable de bibliotecas
Nombre de la historia: Buscar huella dactilar	
Prioridad en el negocio: alta	**Riesgo en desarrollo:** bajo
Puntos estimados: 3	**Iteración asignada:** 1
Programadores responsables: Asistentes de las TIC	
Descripción: quiero eliminar de la base de datos las dos muestras de la huella dactilar capturadas con su respectivo número de cédula.	
Validación: el referencista visualizará el mensaje de confirmación de que la huella dactilar se ha eliminado exitosamente.	

Tabla 3. Historia de usuario "Eliminar huella dactilar"
Fuente: elaboración de las autoras (2024)

Anexo B

La *Tabla 1* muestra la planificación de tareas para este sprint, se tomaron desde la tarea 5 a la tarea 8 del product backlog, las cuales tienen que ver con la instalación del entorno de desarrollo hasta la modificación de código en la interfaz de préstamo del Sistema de Bibliotecas Koha. La lista de tareas de este sprint backlog tiene una duración de 28 días.

Nro.	Tarea	Responsables	Tiempo estimado
5	Instalación del entorno de desarrollo	Asistente de TIC	10
6	Generación de código para el funcionamiento de la interfaz de autenticación biométrica	Asistente de TIC	10
7	Conexión de la interfaz de autenticación con el motor de base de datos MySQL	Asistente de TIC	3
8	Modificación de código en la interfaz de préstamo del Sistema de Bibliotecas Koha	Asistente de TIC	5
		Total	28

Tabla 1. Tareas del segundo sprint
Fuente: elaboración de las autoras (2024)

Tercer sprint

La *Tabla 2* muestra la planificación de tareas para este sprint, se tomaron desde la tarea 9 a la tarea 10 del product backlog, las cuales tienen que ver con la implementación de la interfaz de autenticación biométrica hasta las pruebas de unidad respectivas. La lista de tareas de este sprint backlog tiene una duración de 12 días.

Nro.	Tarea	Responsables	Tiempo estimado
9	Implementación de la interfaz de autenticación biométrica	Asistente de TIC	7
10	Pruebas de unidad	Asistente de TIC	5
		Total	12

Tabla 2. Tareas del tercer sprint
Fuente: elaboración de las autoras (2024)

Cuarto sprint

La *Tabla 3* muestra la planificación de tareas para este sprint, se tomaron desde la tarea 11 a la tarea 12 del product backlog, las cuales tienen que ver con la integración de la interfaz de autenticación biométrica con el módulo de préstamo del Sistema de Bibliotecas hasta las pruebas de integración respectivas. La lista de tareas de este sprint backlog tiene una duración de 12 días.

Nro.	Tarea	Responsables	Tiempo estimado
11	Integración de la interfaz de autenticación biométrica con el módulo de préstamo del Sistema de Bibliotecas	Asistente de TIC	7
12	Pruebas de integración	Asistente de TIC	5
		Total	12

Tabla 3. Tareas del tercer sprint
Fuente: elaboración de las autoras (2024)

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Anexo C

Prueba de unidad	
Número de caso de prueba: 2	**Número de historia de usuario:** 2
Nombre de caso de prueba: Registrar huella dactilar	
Descripción: se almacenan las dos muestras de la huella dactilar del usuario en la base de datos. **Pasos de ejecución:** 1. Permanecen visualizadas las muestras de la huella dactilar capturadas. 2. Se presiona el botón Registrar. 3. Se ingresa el número de cédula del usuario. 4. Se muestra un mensaje de confirmación de registro exitoso.	
Resultado esperado: la aplicación almacena en la base de datos las dos muestras de huella dactilar capturadas por el dispositivo biométrico asociadas al número de cédula del usuario.	**Resultado obtenido:** la aplicación ha almacenado exitosamente las muestras de huella dactilar asociadas al número de cédula del usuario y presenta el mensaje de confirmación.
Acciones correctivas: ninguna	
Evaluación: correcta	

Tabla 1. Caso de prueba "Registrar huella dactilar"
Fuente: elaboración de las autoras (2024)

Prueba de unidad	
Número de caso de prueba: 3.1	**Número de historia de usuario:** 3
Nombre de caso de prueba: Buscar huella dactilar cuando existe	
Descripción: captura una muestra de huella dactilar del usuario y realiza la búsqueda en la base de datos; en caso de ya existir retorna como respuesta el número de cédula. **Pasos de ejecución:** 1. Se muestra la pantalla principal de la interfaz. 2. El usuario coloca su dedo índice sobre el lector de huellas dactilares. 3. Se presiona el botón Buscar 4. Se visualiza la muestra de la huella dactilar capturada. 5. Se muestra el número de cédula del usuario a través de un cuadro de diálogo.	
Resultado esperado: la aplicación presenta el número de cédula del usuario a través de un cuadro de diálogo.	**Resultado obtenido:** la aplicación ha mostrado el número de cédula del usuario asociado a la huella dactilar capturada a través de un cuadro de diálogo y presenta la huella dactilar en la interfaz de autenticación biométrica.
Acciones correctivas: ninguna	
Evaluación: correcta	

Tabla 2. Caso de prueba "Buscar huella dactilar cuando existe"
Fuente: elaboración de las autoras (2024)

Prueba de unidad	
Número de caso de prueba: 3.2	**Número de historia de usuario:** 3
Nombre de caso de prueba: Buscar huella dactilar cuando no existe	
Descripción: captura una muestra de huella dactilar del usuario y realiza la búsqueda en la base de datos; en caso de no existir presenta el mensaje "Cédula no registrada". **Pasos de ejecución:** 1. Se muestra la pantalla principal de la interfaz. 2. El usuario coloca su dedo índice sobre el lector de huellas dactilares. 3. Se presiona el botón Buscar. 4. Se visualiza la muestra de la huella dactilar capturada. 5. Se muestra el mensaje "Cédula no registrada".	
Resultado esperado: la aplicación presenta el mensaje "Cédula no encontrada" en un cuadro de diálogo.	**Resultado obtenido:** la aplicación presenta un mensaje indicando que la cédula de identidad asociada a la huella dactilar capturada no fue encontrada.
Acciones correctivas: ninguna	
Evaluación: correcta	

Tabla 3. Caso de prueba "Buscar huella dactilar cuando existe"
Fuente: elaboración de las autoras (2024)

Prueba de unidad	
Número de caso de prueba: 4.1	**Número de historia de usuario:** 4
Nombre de caso de prueba: Buscar huella dactilar cuando no existe	
Descripción: elimina las dos muestras de huella dactilar del usuario y el número de cédula del usuario asociado, en caso de existir, de la base de datos. **Pasos de ejecución:** 1. Se muestra la pantalla principal de la interfaz. 2. El usuario coloca su dedo índice sobre el lector de huellas dactilares. 3. Se presiona el botón Eliminar. 4. Se visualiza la muestra de la huella dactilar capturada. 5. Se muestra el mensaje "Se ha eliminado el registro exitosamente".	
Resultado esperado: la aplicación elimina las dos muestras de huella dactilar capturadas por el dispositivo biométrico y el número de cédula asociado de la base de datos.	**Resultado obtenido:** la aplicación ha eliminado exitosamente las dos muestras de huella dactilar capturadas por el dispositivo biométrico y el número de cédula asociado de la base de datos.
Acciones correctivas: ninguna	
Evaluación: correcta	

Tabla 4. Caso de prueba "Buscar huella dactilar cuando existe"
Fuente: elaboración de las autoras (2024)

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Prueba de unidad	
Número de caso de prueba: 4.2	**Número de historia de usuario:** 4
Nombre de caso de prueba: Buscar huella dactilar cuando no existe	
Descripción: captura una muestra de huella dactilar del usuario y realiza la búsqueda en la base de datos; en caso de no eliminarla, muestra "No se ha podido eliminar el registro". **Pasos de ejecución:** 1. Se muestra la pantalla principal de la interfaz. 2. El usuario coloca su dedo índice sobre el lector de huellas dactilares. 3. Se presiona el botón Eliminar. 4. Se visualiza la muestra de la huella dactilar capturada. 5. Se muestra el mensaje "No se ha podido eliminar el registro".	
Resultado esperado: la aplicación no puede eliminar de la base de datos las dos muestras de huella dactilar capturadas por el dispositivo biométrico puesto que no han sido registradas.	**Resultado obtenido:** la aplicación presenta un mensaje indicando que el registro no ha podido eliminarse.
Acciones correctivas: ninguna	
Evaluación: correcta	

Tabla 5. Caso de prueba "Buscar huella dactilar cuando existe"
Fuente: elaboración de las autoras (2024)

Anexo D

Caso de prueba
Número de caso de prueba: 2
Nombre de caso de prueba: Registrar huella dactilar
Descripción: las dos muestras de la huella dactilar del usuario se almacenan en la base de datos. **Pasos de ejecución:** 1. Permanecen visualizadas las muestras de las huellas dactilares capturadas. 2. Se presiona el botón Registrar. 3. Se ingresa el número de cédula del usuario. 4. Se muestra un mensaje de confirmación de registro exitoso.
Resultado esperado: el sistema almacena las dos muestras de huella dactilar capturadas por el dispositivo biométrico asociadas al número de cédula del usuario en la base de datos.
Resultado obtenido: el sistema ha almacenado exitosamente las muestras de huella dactilar asociadas al número de cédula del usuario y presenta el mensaje de confirmación.
Evaluación: correcta

Tabla 1. Caso de prueba "Registrar huella dactilar"
Fuente: elaboración de las autoras (2024)

Caso de prueba
Número de caso de prueba: 3.1
Nombre de caso de prueba: Buscar huella dactilar cuando existe
Descripción: captura una muestra de huella dactilar del usuario y realiza la búsqueda en la base de datos; retorna como respuesta el número de cédula, accede a la página de préstamos de Koha enviando el número de cédula como parámetro en el enlace. **Pasos de ejecución:** 1. Se muestra la pantalla principal de la interfaz. 2. El usuario coloca su dedo índice sobre el lector de huellas dactilares. 3. Se presiona el botón Buscar. 4. Se visualiza la muestra de la huella dactilar capturada. 5. Se inicia el navegador predeterminado de la máquina cliente. 6. Accede a la página de préstamos del Sistema de Bibliotecas Koha con la cédula de identidad del usuario como parámetro en el URL. 7. Se busca el usuario en Koha por el número de cédula enviado. 8. Realizar el proceso de préstamo en Koha.
Resultado esperado: el sistema envía a Koha el número de cédula del usuario buscado.
Resultado obtenido: el sistema presenta la huella dactilar en la interfaz de autenticación biométrica y ha enviado el número de cédula del usuario asociado a la huella dactilar capturada al Sistema de Bibliotecas Koha.
Evaluación: correcta

Tabla 2. Caso de prueba "Buscar huella dactilar cuando existe"
Fuente: elaboración de las autoras (2024)

Caso de prueba
Número de caso de prueba: 3.2
Nombre de caso de prueba: Buscar huella dactilar cuando existe
Descripción: captura una muestra de la huella dactilar del usuario y realiza la búsqueda en la base de datos; en caso de no existir, presenta el mensaje "Cédula no registrada". **Pasos de ejecución:** 1. Se muestra la pantalla principal de la interfaz. 2. El usuario coloca su dedo índice sobre el lector de huellas dactilares. 3. Se presiona el botón Buscar. 4. Se visualiza la muestra de la huella dactilar capturada. 5. Se muestra el mensaje "Cédula no registrada".
Resultado esperado: el sistema presenta el mensaje "Cédula no encontrada" en un cuadro de diálogo.

DOI: http://dx.doi.org/10.22201/iibi.24488321xe.2025.103.58968

Resultado obtenido: el sistema ha mostrado un mensaje indicando que la cédula de identidad asociada a la huella dactilar capturada no ha logrado encontrarse.
Evaluación: correcta

Tabla 3. Caso de prueba "Buscar huella dactilar cuando existe"
Fuente: elaboración de las autoras (2024)

Caso de prueba
Número de caso de prueba: 4.1
Nombre de caso de prueba: Buscar huella dactilar cuando existe
Descripción: elimina de la base de datos las dos muestras de huella dactilar del usuario y el número de cédula del usuario asociado en caso de existir. **Pasos de ejecución:** 1. Se muestra la pantalla principal de la interfaz. 2. El usuario coloca su dedo índice sobre el lector de huellas dactilares. 3. Se presiona el botón Eliminar. 4. Se visualiza la muestra de la huella dactilar capturada. 5. Presenta el mensaje "Se ha eliminado el registro exitosamente".
Resultado esperado: el sistema elimina de la base de datos las dos muestras de huella dactilar capturadas por el dispositivo biométrico y el número de cédula asociado.
Resultado obtenido: el sistema ha eliminado exitosamente de la base de datos las dos muestras de huella dactilar capturadas por el dispositivo biométrico y el número de cédula asociado.
Evaluación: correcta

Tabla 4. Caso de prueba "Buscar huella dactilar cuando existe"
Fuente: elaboración de las autoras (2024)

Caso de prueba
Número de caso de prueba: 4.2
Nombre de caso de prueba: Buscar huella dactilar cuando no existe
Descripción: captura una muestra de huella dactilar del usuario y realiza la búsqueda en la base de datos; en caso de no eliminarla, muestra "No se ha podido eliminar el registro". **Pasos de ejecución:** 1. Se muestra la pantalla principal de la interfaz. 2. El usuario coloca su dedo índice sobre el lector de huellas dactilares. 3. Se presiona el botón Eliminar. 4. Se visualiza la muestra de la huella dactilar capturada. 5. Presenta el mensaje "No se ha podido eliminar el registro".

Resultado esperado: el sistema no puede eliminar de la base de datos las dos muestras de huella dactilar capturadas por el dispositivo biométrico puesto que no han sido registradas.
Resultado obtenido: el sistema ha mostrado un mensaje indicando que el registro no ha podido eliminarse.
Evaluación: correcta

Tabla 5. Caso de prueba "Buscar huella dactilar cuando existe"
Fuente: elaboración de las autoras (2024)