UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Vínculos

http://revistas.udistrital.edu.co/ojs/index.php/vinculos

Revista VÍNCULOS
Ciencia, Tecnología y Sociedad: Un Enlace hacia el Futuro

I+D Investigación y Desarrollo

Desarrollo prototipo de un sistema de información biométrico dactilar

Development prototype of a biometric information system dactilar

Abdúl M. Reyes Parra[1] Fredy A. Verástegui González[2] Jesus A. Collazos Sánchez[3]

Para citar este artículo: A. M. Reyes, F. A. Verástegui y J. A. Collazos, "Desarrollo prototipo de un sistema de información biométrico dactilar". *Revista Vínculos: Ciencia, Tecnología y Sociedad*, vol 15, n° 2, julio-diciembre 2018, 29-40. DOI: https://doi.org/10.14483/2322939X.13946.

Recibido: 09-03-2018 / Aprobado: 12-06-2018

Resumen

En el presente artículo se especifica el desarrollo de un prototipo de sistema de información biométrico dactilar (PSIBID) y su utilización como herramienta tecnológica para el control de acceso y registro de usuarios en la Universidad de la Amazonia. Para su desarrollo se optó por la utilización de tecnologías abiertas que permiten modular su funcionamiento a los procesos y necesidades identificados en los requerimientos de la universidad, estas tecnologías, como el sensor biométrico dactilar FMP10A, permiten realizar cambios en su protocolo de trato de datos biométricos; en este caso, la captura de imagen dactilar se lleva a cabo de manera local limitado a 165 registros que pueden ser almacenados en su memoria flash, restringiendo su uso e implementación. En este trabajo, se agregan funciones adicionales, permitiendo la extracción de datos, comunicación y validación de estos gracias a la centralización de los procesos.

Palabras clave: biométrico, imagen dactilar, Raspberry Pi 3, sensor óptico, servicio web, servidores.

Abstract

This article specifies the development of a system prototype of fingerprint biometric information (SPFBI). Furthermore, it can use as a technological tool so as to access control and user registration in the Amazonia University. To achieve this project, it was decided to use open technologies that allow to modulate its operation to the processes and needs identified in the requirements of the University, these technologies and the fingerprint biometric sensor FMP10A allow us to make changes in its biometric data treatment protocol, in this case, fingerprint capture, a process carried out locally limited to 165 records that can be stored in its flash memory, thus restricting its use and implementation. In this project, additional functions are added, allowing the extraction of data, communication and validation of them. It can be possible because of the centralization of the processes.

Keywords: biometric, fingerprint, Raspberry Pi 3, optical sensor, web service, servers.

1. Normalista Superior, Escuela Normal Superior. Afiliación institucional Universidad de la Amazonia, Correo electrónico: mauricio0121@gmail.com, abd.reyes@udla.edu.co
2. Magíster en Ciencias de la Información y las Comunicaciones, Universidad Distrital Francisco José de Caldas. Afiliación institucional Universidad de la Amazonia. Correo electrónico: f.verastegui@udla.edu.co
3. Estudiante Universidad de la Amazonia. Correo electrónico: je.collazos@udla.edu.co

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

1. Introducción

Hoy día, con el avance de las nuevas tecnologías, se busca una implementación modular que supla necesidades de las diferentes organizaciones en la mejora de procesos relacionados con seguridad, control y registro, lo cual garantice un funcionamiento acorde a sus requerimientos. El objetivo planteado del PSIBID es implementar tecnologías abiertas de bajo costo que influyan en la modernización de control de acceso a los diferentes espacios de la universidad en la que se realizarán las pruebas y adaptación, de esta forma se apoya la seguridad y el control de ingreso del personal.

Los sistemas de información con sus limitaciones artificiales, naturales, de entorno, entradas y salidas se definen en 2011; así, desde una perspectiva técnica, un sistema de información recopila, almacena y difunde información del entorno de una organización y las operaciones internas para apoyar funciones y toma de decisiones, comunicación, coordinación, control, análisis y visualización [1]. Los sistemas de información transforman los datos sin procesar en información útil a través de tres actividades básicas: entrada, procesamiento y salida. Se identifican entonces los componentes de *hardware* y *software* que interactúan entre sí, definiendo el modo de funcionamiento del PSIBID y brindando la información necesaria para la toma de decisiones, basándose en datos obtenidos para el procesamiento de imágenes y definición en políticas de optimización y administración. Es con base en lo anterior que surge importancia de la biometría dactilar, la cual juega un rol significativo en el propósito de identificación de usuarios a los que se les habilite el acceso a las dependencias de la Universidad de la Amazonia, tales como: salas de computo, laboratorios, áreas administrativas y demás espacios en los que sea requerido implementar este tipo de solución, limitando la intromisión de personas no autorizadas que puedan provocar algún tipo de daño o perturbación en el normal funcionamiento y ejecución de las actividades.

Por lo mencionado anteriormente se identifican las condiciones que favorecen su implementación como lo son perdurabilidad (no presenta variaciones en los usuarios al transcurrir el tiempo), cuantificación (se puede expresar numéricamente) [2-3], unicidad (identificador único para cada usuario) y universalidad (todos los usuarios la poseen) [4]. Al tener como parámetro que cumple con las condiciones anteriores, se procede a definir las categorías de procesamiento biométrico dactilar que se aplican en el proyecto, como lo son identificación y autentificación.

La categoría de identificación *Automated Fingerprint Identification System* (AFIS), consiste en conocer solo la imagen de la huella dactilar y compararla con las existentes en la base de datos para hallar la identidad de la persona a la que pertenece (1:N). ; por otro lado, la autenticación (1:1) consiste en obtener la imagen de la huella dactilar de una persona —de la cual se conoce su identidad— para compararla con la que se almacena en la base de datos y verificar si la huella dactilar le pertenece [5]. En pocas palabras, AFIS cambia la forma en la que los expertos en huellas dactilares realizan las comparaciones, ya que para declarar una coincidencia (autentificación) no se lleva a cabo la misma tarea que se realizaba antes del uso de las BD o BD automatizadas [6].

Al definir los factores de ejecución y funcionamiento con la descripción suministrada, es necesario que el PSIBID supla las necesidades de fiabilidad, respuesta, durabilidad, adaptabilidad, innovación, practicidad y otros factores intervinientes, los cuales permiten establecer en tiempo real la plena identidad de los usuarios que pertenecen o ingresan a la universidad y hacer uso de las instalaciones. Esto es posible sin tener que recurrir a soluciones obsoletas para la validación de información como llaves, tarjetas o contraseñas, pues es ahí cuando el sistema desarrollado permite el acceso basado en huella dactilar; su implementación y distribución genera como valor agregado el control de etapas de desarrollo e implementación en tanto facilitan futuros cambios dependiendo de la necesidad que sobrevenga.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

2. Metodología y desarrollo del PSIBID

En el presente artículo se discute el dominio relacionado con el desarrollo, se explica la visión general del sistema de información propuesto (en este caso PSIBID), las consideraciones de diseño, *hardware* (facilidad de adquisición), *software* (portabilidad, practicidad, leguaje de programación y fácil acceso a la información), funciones, mejoras, integración, políticas de administración y optimización [7].

2.1 Desarrollo evolutivo

La contextualización de la idea general en este modelo es el desarrollo de un sistema inicial, el cual se expone de manera premeditada a los comentarios de los usuarios, clientes o representantes, permitiendo la experimentación con el sistema inicial, de esta forma podrán retroalimentar en N veces hasta lograr el desarrollo óptimo y su refinamiento [8]. Al ser catalogada como metodología ágil, se centra en las interacciones, la duración de cada iteración es de dos semanas a un mes y cada se completa con el resultado de una versión pequeña del producto en estado de desarrollo [9]. Lo que convierte en ventaja a este modelo sobre otros es obtener acceso anticipado a la realimentación de información, además de ejecutar las actividades de especificación, desarrollo y pruebas en cada interacción de la metodología como se observa en la Figura 1.

Figura 1. Modelo de desarrollo evolutivo [8].

2.1.1 Diseño bosquejos iniciales del PSIBID

Se diseñan bosquejos en los cuales se visualizan los elementos que serán parte fundamental del funcionamiento del PSIBID como conexión a BD, consumir un servicio web, utilizar algún tipo de dispositivo, conexión a red y otros. Estos bosquejos y su descripción proveerán un contexto que no se aleje de la realidad del diseño final, brindando un mayor entendimiento por parte del cliente y los desarrolladores (Figura 2 y Figura 3).

Un componente clave de los sistemas de información es la monitorización constante, esto ayuda a detectar y definir problemas que se puedan presentar; de esta forma, permite proporcionar una base oportuna de acciones a seguir, lo que permite dar prioridad a la calidad y veracidad de la información que suministre el sistema PSIBID [10].

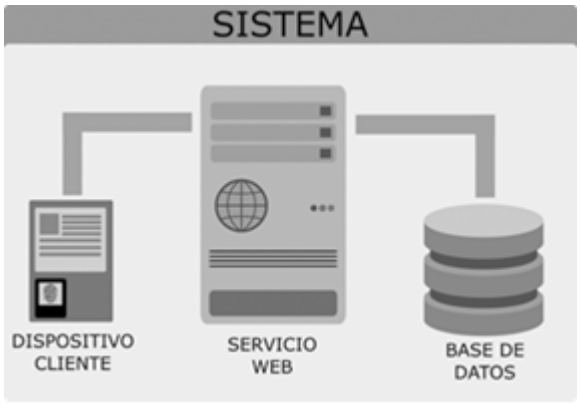

Figura 2. Modelo de desarrollo evolutivo
Fuente: elaboración propia.

Figura 3. Bosquejo PSIBID
Fuente: elaboración propia.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

2.1.2 Desarrollo de la temática

Se especifica el análisis de requerimientos y ajustes por parte del cliente (universidad) relacionados con el desarrollo del proyecto, se documenta de manera clara y precisa (funcionalidad, rendimiento, restricciones de diseño y atributos de calidad) un software y sus interfaces externas [11].

2.1.3 Desarrollo

El desarrollo se basa en diferentes principios que parten desde la temática, plataformas tecnológicas, documentación y diseño de producto, incluyendo actividades pertenecientes a la parte de desarrollo y pruebas [12]. En el desarrollo del PSIBID se identifican cambios en el diseño que son implementados y probados, asegurando el mejoramiento y cumplimiento de su desarrollo respecto a los requerimientos; por tal motivo, se generaron versiones intermedias permitiendo que el cliente pudiese visualizar e interactuar con ellas, garantizando así el desarrollo y cumplimiento de las expectativas, anexando requerimientos o mejoras según sea el caso.

2.1.4 Validación parcial

En esta fase el diseño y desarrollo del PSIBID se encuentra en la validación parcial, ya que se generaron más solicitudes por parte del cliente —en este caso la Universidad de la Amazonia— en la que se procederá a anexar funciones que mejoren el control de acceso a los espacios físicos, permitiendo control en tiempo real; en ese orden de ideas, se pasa a retroalimentar todo el proceso y ajustar mejoras significativas para el futuro del proyecto, permitiendo su modulación evolutiva y dando un valor agregado como solución adaptativa a futuras necesidades.

2.2. Hardware principal del PSIBID

El *hardware* utilizado se divide en dos dispositivos principales para el desarrollo del PSIBID. El FPM10A, sensor biométrico dactilar encargado de registrar y comparar los datos de los usuarios, el cual estará conectado por *jumpers* y un serial USB a una Raspberry Pi 3 en la que se ejecutará la aplicación cliente encargada de simular el funcionamiento y control del sensor biométrico dactilar, existiendo la posibilidad de utilizarse como interfaz de comunicación en los dos dispositivos ya mencionados.

El sensor óptico biométrico dactilar que se observa en la Figura 4, estructura su funcionamiento en absorber la luz al momento de realizar la captura de la huella cuando el dedo toca la superficie del lector, generando un *buffer* de imagen de las crestas donde se produce una reflexión total. La luz resultante y las zonas de oscuridad permiten el registro de una huella dactilar que será procesada por dos *buffers* de caracteres, los cuales almacenan los modelos de la plantilla en la memoria *flash*, esta última tendrá una capacidad de almacenaje en este modelo de 162 plantillas dactilares con un tamaño cada una de 256 x 256 pixeles [13].

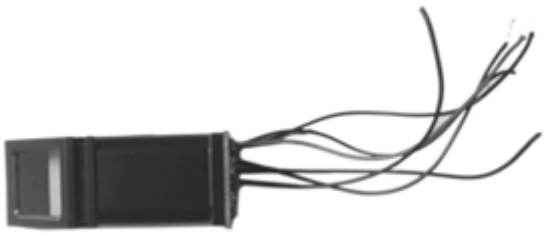

Figura 4. Sensor óptico biométrico dactilar FPM10A.
Fuente: elaboración propia.

La Raspberry Pi 3 que aparece en la Figura 5 es denominada una computadora de pequeño tamaño con buenas prestaciones gracias a su buen número de puertos GPIO (*general input/output*), permite hacer uso de ellos para diferentes dispositivos modulares. Como una pantalla TFT (siglas en inglés de transistor de películas finas) capacitiva en la que se visualizará la aplicación cliente, permitiendo la interacción de los usuarios con el sensor biométrico. Su sistema operativo está basado en una distribución Linux conocida como Debian, la cual, a su vez, se modifica para un funcionamiento optimizado con

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

la arquitectura de la Raspberry Pi 3 que adopta el nombre de Raspbian, este tiene instalado por defecto el intérprete de Python para ejecución de la aplicación cliente que permite la comunicación con el sensor biométrico [14].

Figura 5. Raspberry Pi 3.
Fuente: elaboración propia.

2.3 Arquitectura *software* del PSIBID

La arquitectura consiste en aplicación cliente, servicio web, base de datos. En la Figura 6 se observa el diagrama de flujo en el que se basa el desarrollo del PSIBID, su ejecución y procesos, adaptándolos a las necesidades del proyecto.

Figura 6. Diagrama de flujo de interacción del PPSIBID.
Fuente: elaboración propia.

En la Figura 7 se muestra la arquitectura del PSIBID en el dispositivo cliente, basada en el modelo de tres capas compuesto de la siguiente forma.

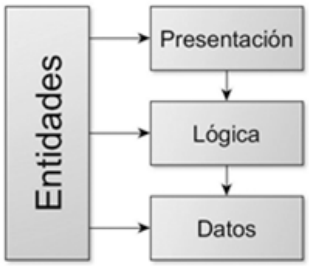

Figura 7. Arquitectura PSIBID en el dispositivo cliente.
Fuente: elaboración propia.

2.3.1 Seguridad

En seguridad, se adoptó el funcionamiento de tres capas permitiendo la adaptación y modulación a la arquitectura del sistema de información misional Chairá. Este sistema es el encargado del manejo de datos implementando las políticas de privacidad de la Universidad de la Amazonia. Las tres capas hacen referencia a la segmentación lógica y física de la arquitectura; en este orden de ideas, se procede a definir las capas usadas en el desarrollo del PSIBID.

- Acceso a dato

Es en esta etapa donde se encuentran almacenados los datos que alimentan al sistema, lo que permite disponer de estos para el cumplimiento de una tarea específica; por tal motivo, al tener acceso a datos necesarios para el funcionamiento correcto del PSIBID, se optó por crear una BD intermedia que permite tomar datos necesario y anexar los propios que sean requeridos, disminuyendo de este modo la pérdida de tiempo en el proceso de migración y adaptación de datos, permitiendo garantizar la totalidad de la información histórica. Lo anterior es posible en tanto el sistema desarrollado se anexa como un módulo en el sistema misional Chairá de la Universidad de la Amazonia.

- Lógica de negocio

Para el desarrollo de esta fase se requirió el trabajo conjunto de Python y C Sharp. Se eligieron por su facilidad de uso, pues la ejecución de comandos básicos del dispositivo lector de huella es en Python,

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

al igual que la interfaz de interacción en la Raspberry Pi 3; el servicio web se desarrolló en C#, igual que su interfaz de interacción en los computadores de los encargados de asignación de espacios físicos y manejo de horarios. La modulación descrita atrás fue necesaria ya que la universidad implementa toda la arquitectura tecnológica ofrecida por Microsoft.

- Presentación

En esta capa se usa el *framework* Ext.net V3 orientado a la web por su compatibilidad multiplataforma con aplicaciones, no es necesario que se descarguen, instalen o configuren, lo que permite disminución de requerimientos de funcionamiento. También se hace uso de la librería de Python Kivy, proporcionando múltiples factores favorables de ejecución al ser multiplataforma, contar con una comunidad amplia y documentación suficiente para ser considerada como una herramienta necesaria para la capa de presentación del PSIBID.

2.3.2 Seguridad a nivel de comunicación

En la comunicación del PSIBID se maneja servicio web, encargado de permitir que tanto los módulos internos como los sistemas externos puedan comunicarse de forma distribuida bajo acoplamiento y de forma transparente, independientemente de su ubicación, lenguaje de desarrollo y plataforma *hardware* [15-17]. También se usa la certificación SSL, la cual permite la utilización de datos biométricos garantizando su privacidad, mientras el protocolo *Secure Socket Layer* (SSL) se puede usar para establecer una comunicación más segura [18-20].
El directorio activo (AD, por sus siglas en inglés) se encarga de proporcionar registro de usuario, autenticación de inicios de sesión de usuarios, escritorio en la nube, máquina virtual incluida administración AD, restricción de acceso a usuarios, servidor de almacenamiento en la nube integrado en la administración de AD y controlar el acceso de usuarios al almacenamiento [19]. Por último, en materia de seguridad el *Advanced Encryption Standard* (AES) es un cifrado de bloques de 128 bits que encripta y descifra la información, el cifrado simétrico también se denomina cifrado de clave privada, ya que se utiliza tanto el en receptor como en el remitente [18]. Estas implementaciones son necesarias para cumplir los estándares de manejo de datos en su comunicación, en este caso, el PSIBIS y el servidor (sistema misional Chairá).

2.3.3 Lenguaje usado para el desarrollo

Para el desarrollo de la aplicación cliente se eligió el lenguaje de programación Python por sus ventajas en la versatilidad, permitiendo programación de bajo, medio o alto nivel, necesarios para el desarrollo del PSIBID. En este trabajo se utiliza para el desarrollo de la interfaz gráfica la librería Kivy de Python de código abierto, específicamente para desarrollo *software* de aplicaciones *multitouch* con una interfaz de usuario natural (NUI, por sus siglas en inglés), que proporciona herramientas necesarias para la interacción del usuario y el dispositivo, permitiendo la comunicación entre el lector de huella y el dispositivo Rasberry Pi 3, modulando su uso con la librería PySerial sobre la que se encuentra gran documentación.

2.3.4 Gestor de BD seleccionado

La estructuración de la base de datos se realizó en Mysql y consta de tablas que almacenan registros de los usuarios y una miniestructura de las dependencias de la Universidad de la Amazonia, la cual permita visualizar información que no esté alejada de la realidad; en este caso, se manejan las siguientes tablas: maestros, estudiantes, administrativos, espacios físicos, horarios y más información que permita el funcionamiento del PSIBID. Este sistema gestor de BD se selecciona por ser rápido, fácil de implementar y contar con una cantidad considerable de complementos, documentación y comunidad de soporte.

2.3.5 Metodología de implementación

La metodología implementada en el PSIBID propuesto utiliza la identificación de huellas dactilares,

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

la autenticación del usuario y registros existentes en la base de datos recolectados (registro de usuarios), se comunicará con la aplicación cliente de la Raspberry Pi 3 por medio de un servicio web. La aplicación cliente, será la encargada de administrar las funciones del sensor óptico dactilar gracias a las funciones adicionales agregadas a lo largo de la investigación, las cuales se adecuan a las necesidades requeridas. El objetivo es proporcionar permisos de acceso a lugares en los que se implemente el PSIBID por medio de biometría dactilar.

2.4 Funciones estándar

A continuación se enuncian brevemente los procedimientos para el proceso estándar. Los procesos de registro huella dactilar se encuentran en la Figura 8.

- Generar imagen (en *buffer* de imagen).
- Generar mapa de caracteres de la imagen (en *buffer* 1).
- Generar imagen (en *buffer* de imagen).
- Generar mapa de caracteres de imagen (en *buffer* 2).
- Generar modelo o plantilla de la huella (en *buffer* 1 y 2).
- Almacenar en memoria *flash* del lector.

Figura 8. Procesos estándar realizado por el lector óptico.
Fuente: elaboración propia.

Los procesos de autenticación de huella dactilar se encuentran en la Figura 9.

- Generar imagen (en *buffer* de imagen).
- Generar mapa de caracteres de imagen (en *buffer* 1).
- Buscar huella en memoria *flash*.

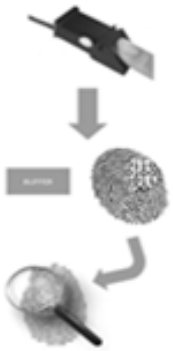

Figura 9. Procesos estándar de autenticación.
Fuente: elaboración propia.

3. Resultados del desarrollo del PSIBID

3.1 Modificación y agregación de procesos estándar del lector óptico biométrico

Al tomar como referencia los procesos estándar del lector óptico biométrico en la Figura 8 y la Figura 9, se evidencia la limitante de trabajo que no se ajusta y modula a las necesidades al centralizar el proceso de manera local, lo que lleva a realizar modificaciones como agregar funciones que se ajusten a las necesidades para el desarrollo adecuado del PSIBID, que permita un manejo y consulta de registros de usuarios, controlando de esta forma accesos y ocupación de espacios de la universidad con información en tiempo real.

En este proceso de registro —que se muestra en la Figura 10— se consigue modificar la ruta de la huella dactilar para no ser almacenada en la memoria *flash* del dispositivo, ya que con el proceso logrado es enviada a la base de datos donde será adicional a la información de los usuarios, ya sean estudiantes, administrativos o docentes.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

Registro con mejoras agregadas al registro de usuarios:

- Generar imagen (en *buffer* de imagen).
- Generar mapa de caracteres de la imagen (en *buffer* 1).
- Generar imagen (en *buffer* de imagen).
- Generar mapa de caracteres de imagen (en *buffer* 2).
- Generar modelo o plantilla de la huella (en *buffer* 1 y 2).
- Leer *buffer* 1 o 2 y almacenar el modelo en la BD.

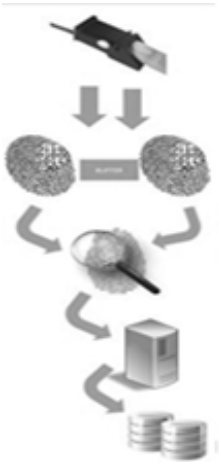

Figura 10. Proceso de registro al agregar funciones y modificar el enrutamiento de los datos biométricos.
Fuente: elaboración propia.

Al momento de autentificar la identidad de un usuario existente en la base de datos se realiza el envío de los datos biométricos de los usuarios que harán uso de las áreas físicas designadas para el desarrollo de las actividades, en este caso podrán ser salas de cómputo, salones de clase, oficinas administrativas, unidad de sistemas, entre otros. Al realizar el envío de los datos realizará el proceso hasta llegar de nuevo en la memoria flash del sensor óptico biométrico para el proceso interno de lectura y autenticación de los usuarios, con una respuesta menor a un segundo para autenticar y validar si pueden hacer uso del espacio físico (Figura 11).

Los procesos de autenticación de usuarios descargando los modelos desde la base de datos se mencionan a continuación.

- Descargar modelo de huella dactilar de BD (en *buffer* 1 o 2).
- Se guarda el modelo de huella en la memoria *flash*.
- Generar imagen (en *buffer* de imagen).
- Generar mapa de caracteres de imagen (en *buffer* 1 o 2).
- Buscar huella en memoria *flash*.

Figura 11. Proceso de autenticación con modificaciones al proceso estándar.
Fuente: elaboración propia.

3.2 Fragmento de código

En este segmento de código se indica el *buffer* que procesa los caracteres, como entradas para comparar con los registros de la memoria *flash*, la condición con la que Python detecte en qué plataforma se estará ejecutando y, finalmente, devuelve una posición diez (tomando en cuenta que el conteo se hace desde cero) que representa el código de respuesta del sensor óptico necesario para la toma de otras decisiones.

```
def GoSearch(buffer):
NoBuffer=int(buffer)
```


ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

```
memoria flash
sisoper=sys.platform
if sisoper=='win32':
ser=serial.Serial('COM3', 57600, timeout=2)
else:
ser = serial.Serial('/dev/ttyUSB0', 57600, timeout=2)
print ser
ser.write(chr(0xEF))
ser.write(chr(0x01))
ser.write(chr(0xFF))
ser.write(chr(0xFF))
ser.write(chr(0xFF))
ser.write(chr(0xFF))
ser.write(chr(0x01))
ser.write(chr(0))
ser.write(chr(0x08))
ser.write(chr(0x04))
ser.write(chr(NoBuffer))
ser.write(chr(0))
ser.write(chr(0))
ser.write(chr(0))
ser.write(chr(0x64))
ser.write(chr(0))
ser.write(chr(0x71+NoBuffer))
print "\nRespuesta de Lector\n"
cadena = ser.read(16)
for i in range (16):
print(hex(ord(cadena[i]))),
ser.close()
return cadena [9].
```

3.3 Carga y descarga de usuarios

El proceso de cargar y descargar usuarios (Figura 12) tiene como eje dos factores fundamentales, el horario de asignación de recurso físico y quiénes son asignados a este; de esta forma, las peticiones de datos por parte del PSIBID se efectúan cuando el sistema lo solicite, permitiendo controlar y prever una saturación o uso concurrente e innecesario de recursos que puedan afectar el funcionamiento del sistema misional Chairá encargado de proveer los datos.
Para hacer claridad en el proceso anteriormente especificado, se procede a detallar su funcionamiento.

- El dispositivo encargado de almacenar y validar la información de usuarios (PSIBID) realizará una petición periódica al servidor sobre quiénes tienen asignación de recursos físicos.
- El servidor, al validar la petición del dispositivo, dará como respuesta el listado de usuarios con su respectivo modelo de huella dactilar que tendrán asignado el acceso en ese horario solicitado.
- Al realizar el proceso de autenticación por parte del o los usuarios, el dispositivo realizara el envío de quien accedió al recurso físico.
- Antes de terminar la actividad designada, sea clase, reunión, charla, préstamo a estudiantes, docentes, administrativos, entre otros, el dispositivo enviará una confirmación final de los usuarios autenticados en el horario de uso establecido y uso del recurso físico.
- Al cumplir el horario de uso del recurso físico, el dispositivo eliminará de su memoria *flash* los datos biométricos de usuarios y realizará los pasos anteriores para autenticar el uso del espacio físico en los horarios siguientes.

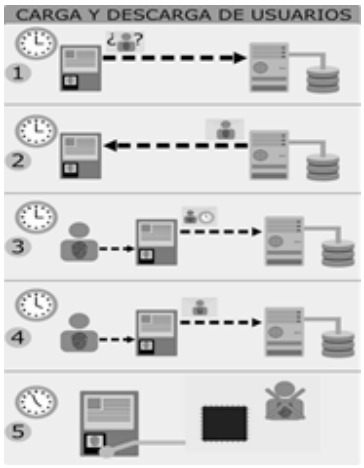

Figura 12. Proceso de carga y descarga de datos de usuarios en horarios de uso de espacios físicos.
Fuente: elaboración propia.

3.4 Interfaz de prueba

La interfaz realizada en Python es muy simple, solo es necesario tener certeza de si los procesos de

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

registro y autenticación funcionan correctamente. El proceso de generación de la interfaz de usuario se propone a partir de una triada conformada por patrón de datos, plantilla de presentación y un modelo de interacción [15].

En la Figura 13 se muestra la interfaz de prueba en la que visualiza la información de la sala como el nombre, materia, docente que la imparte, la opción de ingresar por lectura de huella dactilar. Se tiene como futuro trabajo la modulación de una tarjeta RFID de soporte por si se llegan a presentar fallas en el proceso de autenticación y habilitación de acceso, imágenes de huellas dactilares que se iluminaran si la huella fue encontrada, más un mensaje de información si el proceso presenta error.

Figura 13. Interfaz de prueba del funcionamiento del PSIBID, en la que se realiza en manejo de Reg: registro huella en el sistema, Ent: entrada al espacio físico y Sal: salida.
Fuente: elaboración propia.

4. Conclusiones y trabajos futuros

En este artículo se presenta el desarrollo de un PSIBID en su primera fase de funcionamiento, se especifica el uso de un sensor óptico dactilar (FPM10A) encargado de procesar la información biométrica con algoritmos modificados y adaptados a las necesidades. Esta información biométrica resultante permite la pasarela de datos gracias a la aplicación cliente almacenada en la Raspberry pi3, que se comunica por medio de un servicio web con la BD, en la que se registrará, validará, consultará, inactivará los datos y otros procesos permitidos por el DBA y los parámetros del PSIBID.

Como resultados parciales puede decirse que se logró el almacenamiento externo de la huella dactilar en la BD, la comunicación de la aplicación cliente con el lector biométrico óptico, interacción servicio web, BD y aplicación cliente, permitiendo la identificación de usuarios en tiempo real y generando como valor agregado la modulación del PSIBID a las necesidades de manejo de datos exactos de usuarios que accedan a las instalaciones de la Universidad de la Amazonia, lo anterior sin tener que efectuar cambios de funcionamiento en los procesos al aplicar tecnologías no flexibles a modificaciones que implican un alto costo operacional.

Se propone mejorar el método de funcionamiento por el cual se identifican los horarios de los usuarios que podrán hacer uso de las instalaciones y su identificación al hacer uso del PSIBID para el envío de información a los lectores biométricos cuando esta sea requerida con el fin de autorizar el acceso a los espacios físicos, y borrada de los dispositivos cuando ya no sea necesaria, evitando el incremento de consultas que afecten el funcionamiento de la BD de la universidad y, a su vez, priorizando recursos de los servidores y del sistema para actividades que demanden este tipo de consultas continuas.

Se propone como trabajo futuro la inserción de un módulo RFID para facilitar la identificación de usuarios que puedan presentar inconvenientes con la lectura biométrica de su huella dactilar, generando un reporte que especifique el problema y qué usuario lo presentó; también se anexara un solenoide con funcionamiento de cerradura electrónica inteligente que permita el accionamiento al momento de identificar si el usuario tiene acceso. De igual forma se modulará la información biométrica con la BD de la Universidad de la Amazonia, permitiendo anexar funciones al PSIBID como el control de asistencia y su implementación para el control de acceso a los espacios físicos de la universidad, generando como valor agregado la utilización de tecnologías abiertas

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

que se modulan a las necesidades y requerimientos, facilitando así su implementación y funcionamiento.

Referencias

[1] K. C. Laudon y J. P. Laudon, "Management Information Systems: Managing the Digital Firm", Pearson, 2011.

[2] C. A. Madrigal, J. L. Ramírez, J. C. Hoyos y D. S. Fernández "Diseño de un sistema biométrico de identificación usando sensores ópticos para huellas dactilares", *Revista Facultad de Ingeniería*, n°. 39, 2007, pp. 21–32.

[3] M. Ruiz, C. Rodríguez y J. Olivares "Una mirada a la biometría", *Revista Avances en Sistemas e Informática*, vol. 6, n°. 2, 2009, pp. 29-38.

[4] J. J. Stephan, S. A. Abdullah y R. D. Resan "Use fingerprint technology in developing country security", in IEEE conferences: Annual conference on new trends in information and communications technology applications, 7-9 march, 2017.

[5] P. Komanski, P. T. Higgins, K. M. Higgins y L. K. Fox, "Automated Fingerprint Identification Systems (AFIS)", Elservier Academic Press, 2005.

[6] I. E. Dror y J. L. Mnookin, "The use of technology in human expert domains: challenges and risk arising from the use of automated fingerprint identification system in forensic science", *Law, Probability and Risk*, vol. 9, n°. 1, 2010, pp. 47-67.

[7] C. Saraswat y A. Kumar, "Efficient Automatic Attendance System using Fingerprint Verification Technique, International", *Journal on Computer Science and Engineering,* vol. 2, n°. 2, 2010, pp 264-269.

[8] P. Letelier, "Desarrollo de sistemas de información", Departamento de sistemas de Información y Computación, Universidad Politécnica de Valencia, 2003.

[9] E. Chowdhury, A. B. Hasibul y S. Rahim: "Analysis of the Veracities of Industry Used Software Development Life Cycle Methodologies" Cornell university Library, 2018.

[10] S. Okami y N. Kohtake: "Transitional Complexity of Health Information System of Systems: Managing by the Engineering Systems Multiple-Domain Modeling Approach", in Annual IEEE International Systems Conference (SysCon), Montreal, Canadá, abril 24-27, 2017.

[11] A. N. Camacho, "Herramienta para el análisis de requerimientos dentro de la pequeña empresa desarrolladora de software en Bogotá", Tesis de grado, Facultad de Ingeniería, Pontificia Universidad Javeriana, Bogotá D.C., 2007.

[12] J. V. Reyes , "Propuesta de Modelo para el desarrollo de aplicaciones "TIC" para la Facultad Tecnológica de la Universidad Distrital Francisco José de Caldas", Tesis de maestría, Facultad de Ingeniería, Universidad Distrital Francisco José de Caldas, Bogotá D.C., 2017.

[13] I. C. Cóndor y C. A. Paredes, "Implementación de un Sistema de acceso electrónico mediante la huella dactilar y una clave de acceso", Monografía de grado, Escuela Politécnica Nacional, Quito, Ecuador, 2009.

[14] R. Del Poso, "Los Orígenes de la Raspberry", 2017 [En línea]. Disponible en: https://rafaeldelpozo.wordpress.com/2017/01/17/los-origenes-de-raspberry-pi/

[15] J. I. Triviño y W. J. Giraldo: "Generación de la Interfaz de Usuario de Negocio a Partir de la Asociación de Patrones de Datos, Plantilla de Presentación y Modelo de Interacción", in IEEE 11 the Colombian Computing Conference (CCC), Popayan, Colombia, 2016.

[16] J. Baidya, T. Saha, R. Moyashir y R. Palit, "Design and implementation of a fingerprint based lock system for shared access", in IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, Nevada, enero 9-11, 2017.

[17] P. Serpa, L. Weitzel y L. Calado, "Iintegration of numerical oceanographic modeling systems via web services", in 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, 2018.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

[18] S. U. Jonwal y P. P. Shingare, "Advanced Encryption Standard (AES) implementation on FPGA with hardware in loop", in International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli, 2017. https://doi.org/10.1109/ICOEI.2017.8300776

[19] W. Wei, Y. Zhang, Y. Lu, P. Gao y K. Mu, "A VDI System Based on Cloud Stack and Active Directory", in 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), Guiyang, 2015, https://doi.org/10.1109/DCABES.2015.45

[20] A. Varriale, P. Prinetto, A. Carelli, P. Trotta, "SEcube (TM): Data at rest and data in motion protection", in: Proceedings of the International Conference on Security and Management (SAM), Las Vegas, Nevada, julio 25-28, 2016.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 15, N° 2 (julio-diciembre 2018). pp. 29-40. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.