Prototype of authentication and strong access control for academic computing rooms

Felipe Andrés Corredor, M.Sc[1] , Wolfang Sebastián Corredor, Ing.[1] y
Javier Eduardo Martínez Baquero, M.Sc[1]
[1]Universidad de los Llanos, Villavicencio, Meta, Colombia, felcorredor@unillanos.edu.co,
wolfang.corredor@unillanos.edu.co, jmartinez@unillanos.edu.co

Abstract– ***The academic institutions that have computer rooms to support their teaching processes, must overcome a series of difficulties in terms of entry, access control and monitoring the use of these spaces. This service presents a high demand and the administrative staff that authenticates, controls and supervises these operations is reduced; and although there are hardware devices and computer applications in the context (biometric locks, room control software), these do not have the capacity to integrate to unify data and act as isolated elements.***

This article presents the development and architecture of a solution alternative for authentication and access control to academic computing rooms, with capacity for future integration with academic processes within the classroom. This was done within the framework of a research project at the Universidad de los Llanos, in Villavicencio (Meta), Colombia.

Keywords- Multifactor authentication, access control, Computer rooms, Information security

Digital Object Identifier (DOI):http://dx.doi.org/10.18687/LACCEI2018.1.1.517
ISBN: 978-0-9993443-1-6
ISSN: 2414-6390

Prototipo de autenticación y control de acceso fuerte para salas de cómputo académicas.

Felipe Andrés Corredor, M.Sc[1], Wolfang Sebastián Corredor, Ing.[1] y
Javier Eduardo Martínez Baquero, M.Sc[1]
[1]Universidad de los Llanos, Villavicencio, Meta, Colombia, felcorredor@unillanos.edu.co,
wolfang.corredor@unillanos.edu.co, jmartinez@unillanos.edu.co

***Abstract*– Las instituciones académicas que disponen de salas de cómputo para apoyar sus procesos de enseñanza, deben superar una serie de dificultades en lo referente al ingreso, control de acceso y seguimiento al uso de estos espacios. Este servicio de las salas de cómputo, presenta una alta demanda y el personal administrativo que autentica, controla y supervisa estas operaciones es reducido; y aunque existen en el contexto dispositivos de hardware y aplicaciones informáticas, (cerraduras biométricas, software de control de salas), estos no tienen capacidad de integrarse para unificar datos y actúan como elementos aislados, impidiendo la toma de decisiones a nivel administrativo y pedagógico.**

Este artículo presenta la arquitectura y desarrollo de un prototipo de sistema distribuido de autenticación y control de acceso a salas de cómputo académicas, con capacidad de integración a futuro con módulos de software para procesos académicos dentro del aula. El cual se realizó en el marco de un proyecto de investigación en la Universidad de los Llanos, en Villavicencio (Meta), Colombia.

***Keywords*—Autenticación multifactor, control de Acceso, Salas de cómputo, seguridad informática,**

I. Introducción

En las instituciones educativas se consolida cada vez más, el uso de las TIC en los procesos de enseñanza –aprendizaje; las instituciones de educación media y universitaria a pesar de estar apostándole a mejorar su capacidad instalada en cuanto a salas de informática para atender la amplia demanda de este servicio, sigue con baja proporción de computadores por número de estudiantes, lo que conlleva a que sus salas de informática presenten altas tasas de uso; sumándole a esta situación que el personal administrativo que supervisa y controla el acceso y uso de las salas, también es reducido.

El presente artículo describe los aspectos de diseño y desarrollo de un sistema de supervisión para el apoyo al proceso pedagógico de clases que se dictan en centros de cómputo y que deberían aplicarse de manera genérica en centros de cómputo académicos, Inicialmente se presenta la descripción del problema, pasando luego a la Autenticación, control de acceso y comunicación de este tipo de sistemas desde una implementación propia de un prototipo que se denominó SASSI. Se describe el desarrollo del modelo implementado, donde se presentan los detalles de diseño, desarrollo y despliegue. El siguiente ítem hace referencia a la discusión, donde se analiza la efectividad de su operación en el laboratorio de tecnologías abiertas del grupo de investigación y finalmente se presentan las conclusiones obtenidas.

II. Descripción del problema

A. *Contextualización*

Las técnicas de control de acceso, aplican mecanismos de refuerzo como el hecho de apoyarse en canales SSL/TLS y captcha de varios niveles de robustez, sin embargo, no garantizan un alto nivel de certeza en cuanto que el usuario que se está autenticando, es quien dice ser; siendo aquí donde la biometría es intrínsecamente superior y toma un papel protagónico, ya que crea un fuerte enlace entre la persona (su cuenta) y su identidad, pues sus rasgos o patrones biométricos no podrán ser compartidos, duplicados o perdidos**[1]**. Según [2], una persona utiliza alrededor de 13 contraseñas en su vida cotidiana. La gestión personal de estas contraseñas se dificulta, más aun cuando algunas son difíciles de memorizar y a menudo son comunicadas a terceras partes. La biometría es capaz de mitigar este problema, de uso y gestión, ya que se omite el uso de contraseñas y centra su actuar en la relación persona/identidad.

Las organizaciones en América Latina, implementan en promedio seis medidas de protección a sus sistemas de cómputo (de las 24 planteadas por la Asociación Colombiana de Ingeniería de Sistemas - ACIS); donde se evidencia que los sistemas de autenticación basados en contraseñas (58,2%) y los sistemas biométricos (33,2%), están en primer y quinto lugar de adopción como mecanismo de protección preferidos por las empresas [3]. De esta manera, es coherente encontrar que la autenticación biométrica ya se usa para dar acceso a las aulas de clase a cada persona específica y además gestionar la asistencia a estas aulas. [4], incluso, actualmente existe una tendencia de uso de autenticación de múltiples factores (contraseñas, biométricos y tokens) para hacer más preciso el proceso de autenticación [5]. Cuando se aplican varios factores de autenticación al usuario; lo que "sabe" (por ejemplo, alguna información secreta como una contraseña), lo que "tiene" (por ejemplo, algo en su posesión, como una

Digital Object Identifier (DOI): http://dx.doi.org/10.18687/LACCEI2018.1.1.517
ISBN: 978-0-9993443-1-6
ISSN: 2414-6390

tarjeta inteligente), y lo que "es", por ejemplo, característica biométrica única tales como huellas dactilares, geometría de la mano o el iris; el esquema de autenticación de usuario se puede considerar altamente seguro. [6] [10].

Existen tecnologías de control de acceso basadas en hardware como Cerradura Inteligente Zwave de Yale y Cerradura Digital Biométrica Shs S705 de Samsung, que no son muy económicas (cuestan en promedio US$600) y no tienen capacidad de integrarse con otros sistemas para unificar datos, actúan como elementos aislados. También existen soluciones de software para hacer seguimiento a salas de informática académicas, como ITALC ® y KONTROL PACK®, las cuales actúan más como entono de escritorio remoto y no como manejadores de eventos, afectando incluso la privacidad del estudiante al momento de usar el computador. En general las herramientas del contexto son componentes específicos que difícilmente pueden intercambiar datos entre sí, no permiten la integración de cada uno de los eventos generados por ellos, algunas operan como cajas negras y no se permite el intercambio de datos para obtener información significativa y estratégica, para sobre ellos tomar decisiones y acciones que sustenten la razón de ser de las salas de informática académicas, que es ayudar a que los procesos de enseñanza/aprendizaje basados en salas de informática y TIC, sean más eficientes, y que el uso de los equipos se oriente estrictamente a los aspectos académicos relacionados con la clase.

B. Problema

Gran cantidad de estudiantes que a su vez demandan el uso de gran cantidad de equipos de cómputo, así como el reducido número de personal administrativo que supervise y controle el acceso y uso de las salas, sumado a la falta de políticas de seguridad (solo se limitan a un reglamento) y la poca inversión en mecanismos que ayuden a mitigar los riesgos asociados, conllevan a un escenario complejo para la docencia y la gestión de informática. Según ACIS, de los 12 sectores económicos que invierten en mecanismos de seguridad y protección, el sector educativo es el cuarto que menos lo hace [3]. La universidad de los Llanos no es ajena a esta situación, cuenta con más de 5600 estudiantes; (5250 pregrado y 392 posgrado) [7] y con 8 salas de informática disponibles a la comunidad estudiantil, alcanzando apenas una proporción de 30 estudiantes por computador. Si a esto se le adiciona que los funcionarios encargados de mantener y dar soporte son apenas 3 auxiliares técnicos y un ingeniero, la proporción se reduce a 1400 estudiantes por personal administrativo de apoyo.

La ejecución de actividades no permitidas (Instalación de Software no autorizado, Juegos, Servicios de Entretenimiento en línea, etc) en las salas de informática de las Instituciones Educativas (IE), es una constante, debido al uso masivo de este servicio por parte de los estudiantes; que dificulta las acciones de Autenticación, control de acceso y supervisión que se deben mantener permanentemente. La falta de control y supervisión permanente a los centros de cómputo, puede llevar a la generación de ataques cibernéticos [8], de lo cual no están exentas las IES (Instituciones de Educación Superior), es más; según la empresa Norton, el porcentaje de millennials (jóvenes entre 20 y 30 años) que han sido víctimas de cibercrímen llega al 70% [7], esta generación cubre gran parte de la población universitaria. Dentro de 20 sectores de la industria, el sector educativo es el octavo con mayor cantidad de incidentes [8].

III. DESARROLLO DEL MODELO

A. Diseño y arquitectura

Este proyecto planteó el diseño y desarrollo de una herramienta computacional para apoyar los procesos pedagógicos en centros de cómputo académicos, la cual fue denominada SASSI; obteniendo para este caso un prototipo constituido por componentes de hardware y una serie de módulos de software, equipos de las salas de computo (clientes) y el servidor, los cuales interactúan a través de una red local aislada y basada en canales cifrados. Necesarios para asumir automaticamente (autenticación, control de acceso y monitorización de eventos) en términos funcionales, jurídicos y de seguridad.

A continuación se presenta la estructura de los módulos de autenticación y control de Acceso, implementados en SASSI.

Módulo de Autenticación

El módulo de Autenticación implementado es multifactor y tiene como propósito validar que el usuario que está ingresando sea quien dice ser, a través de dos factores: lo que el usuario "es" (Biometría) y lo que el usuario "sabe" (Password). [9].

El proceso inicia cuando el Usuario (Profesor) llega a la sala de cómputo y le es solicitada su Huella (*Hu*), la cual es enviada al servidor (*Serv*), a través de un canal cifrado (mediante Sockets SSL). Una vez validada *Hu*, contra la *Hu* almacenada en la BD (*Hu'*), se crea un archivo de *Token'* cuyo contenido es el hash MD5 del usuario (Contiene Informacion del Usuario y datos pseudoaletorios asociados a las marcas de tiempo). Mientras esto sucede, el Cliente i (Cli_i , i<n , donde n=cantidad de salas) solicita el envó del *Token'*, lo cual le será aceptado solo si *Hu=Hu'* y tiene asiganda la sala en el respectivo horario. Finalmente el Cli_i realiza una solicitud web (HTTP_GET) que es validada en *Serv* y le concede acceso a la Sala i (apertura automatica de la puerta de

Sala$_i$) y a registrar las operaciones que se van a realizar dentro de la sala. Ver Figura 1.

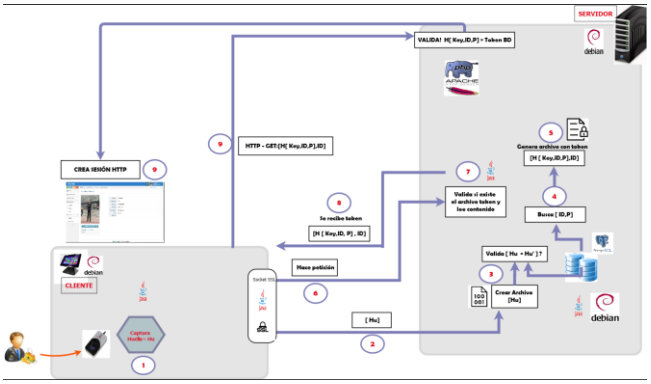

Figura 1. Estructura Módulo Autenticación

Módulo de control de acceso

Este módulo inicia su actuación, una vez ha finalizado el método de autenticación que ya ha garantizado su correcta identidad. El Usuario recibe a través del método HTTP_GET un menú de opciones sobre las herramientas de software que están disponibles para el uso durante la clase que va a iniciar (los cuales se van a monitorizar durante ese periodo).

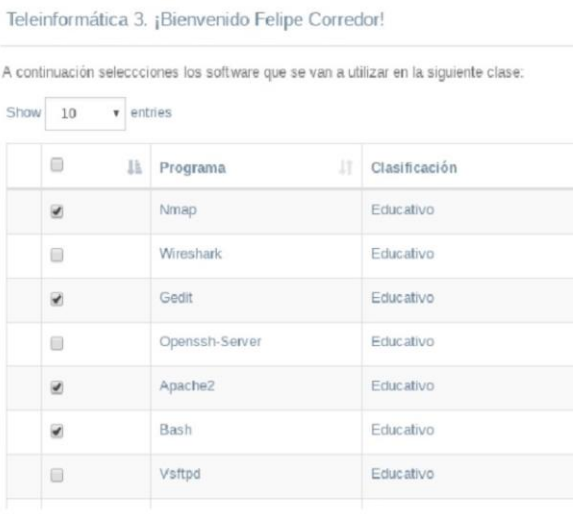

Figura 2. Menú Control de Acceso SASSI - Opciones de software para Clase

Los datos son transmitidos al Servidor SASSI, el cual enviará el comando de activación de los sensores en cada computador de la sala. Posteriormente se da la apertura automática de la puerta de la sala, para el ingreso del Profesor y los Estudiantes. A continuación se representa el módulo de autenticación diseñado:

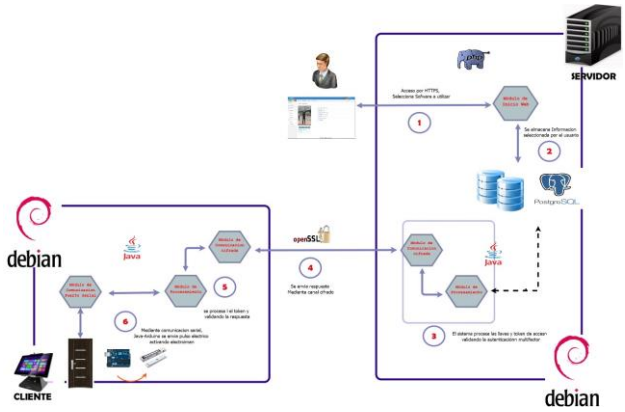

Figura 3. Estructura Módulo Autenticación

La base del proyecto fue desarrollada en el lenguaje de programación JAVA (jdk1.8), apoyándose de su API criptográfica y de comunicaciones, sobre el sistema operativo GNU/Linux (Distribución Debian 9.3). El almacenamiento se realizó mediante el motor de bases de datos Postgres y la comunicación con la API java.net y el servidor web Apache.

TABLA I. TABLA DE TECNOLOGÍAS UTILIZADAS.

Herramienta	Autenticación	Comunicación	Control Acceso
Java 8	X	X	X
CrossMatch SDK Java - Linux	X		
JavaFX	X		
JDBC Driver	X		X
Postgresql 9.4	X		X
Php 5.0	X		
Apache Werb server 2	X	X	
Debian GNU/Linux 9.3	X		
Keytool		X	
Java 8 (SSLSockets) y API Criptográfica		X	
GNU SerialPort (for Java)			X
Raspbian (GNU/Linux) GPIO.			X

B. Descripción de componentes del sistema

Para la implementación de la arquitectura, se eligieron componentes de hardware (Tabla II) capaces de apoyar la automatización de ciertas tareas en cada fase de la autenticación, la comunicación y el control de acceso; así por ejemplo, el lector de huella dactilar realiza la primera fase de autenticación y la raspberry pi junto a la pantalla táctil, realizan la segunda fase.

1	Pantalla táctil.
2	Lector de huella dactilar.
3	cerradura eléctrica.
4	Puerta de madera a escala.
5	Relé estado Solido
6	Computador Cliente
7	Servidor (Contenedor de aplicaciones) / Sistema de autenticacion.
8	Pantalla del servidor.
9	Arduino mega.

Figura 4. Componentes Prototipo SASSI– Fase de prueba.

La figura 4 presenta algunos componentes usados en fase de pruebas, con un escenario simulado, donde se trabajó con una puerta de madera (1 mt de alto x 0,6 mts de ancho) a escala, un servidor y dos clientes (equipos portátiles: uno de ellos con pantalla táctil). A continuación (ver tabla II) se describen los dispositivos usados en la puerta real del acceso a la sala de cómputo de GITECX.

TABLA II.
Dispositivos de Hardware – Puerta de Ingreso a la Sala de cómputo

DISPOSITIVO	CARACTERISTICAS
Equipo de cómputo - cliente	DELL OPTIPLEX 3020 - Procesador Intel® Core™ i5 (3.3 GHZ), Memoria RAM DDR3 8GB, S.O. Debian /GNU/Linux 9.3 (Stretch).
Pantalla táctil	Display: 7", Resolución: 800 x 480 Pixeles, Puerto DSI de conexión a Rapsberry PI Board – Ribbon Cable
Lector de huella	U Are U 4500 Digital Persona
Electroimán	Yale. 600 Lbs, Acero 100%, Con Buzzer
Tarjeta de desarrollo	Procesador: Quad-Core 1.2 GHz Tarjeta MicroSD de 32 GB (clase 10) CanaKit 2.5A fuente de alimentación con 5 pies Micro USB Cable y filtro de ruido (por UL)

Fuente: Elaboración propia

El proceso de construcción e implementación en el entorno real de operación de SASSI (Acceso a centro de cómputo de GITECX), incluyó el circuito controlador de apertura desde el interior, y el controlador de autenticación y acceso, que permite la apertura automática de la puerta metálica. A continuación se presenta la vista frontal y posterior de cada controlador implementado (ver figura 5 y figura 6).

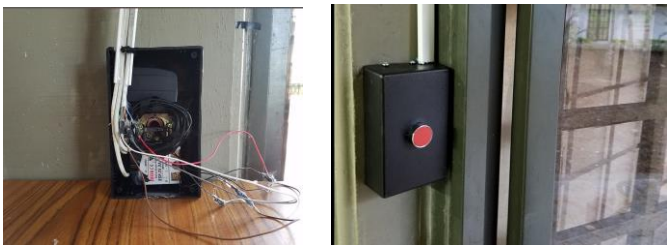

Figura 5. Controlador Apertura Interna de SASSI– Laboratorio GITECX

Figura 6. Controladora de Autenticación y Acceso, SASSI – Laboratorio GITECX

IV. Discusión

El prototipo del sistema SASSI fue adecuado en el laboratorio de tecnologías abiertas del grupo de investigación, en el cual se establecieron casos de análisis y validación de parámetros sobre el diseño.

Se cargaron dos cursos del programa de ingeniería de sistemas de la universidad de los Llanos, denominados estructuras de datos (602301) de tercer semestre y teleinformática III (602001) de décimo semestre. Verificando la autenticación de los profesores de cada curso (usuarios: eperez y fcorredor) y dando apertura a la puerta en el horario registrado.

Figura 7. Estructura Módulo Autenticación y Control de Acceso / SASSI - Laboratorio GITECX

El módulo de autenticación logró validar cada usuario contra la base de datos, serializando el password a través del Crossmatch SDK Digital persona (formato definido en ISO/IEC 17794-2 : 2005) y enviándolo según lo descrito en el ítem *Módulo de autenticación*.

El módulo de control de acceso solicitó los cursos a cada usuario y procedió a dar apertura a la puerta:

Curso	**Software Disponible**	**Software Seleccionado**
Estructuras de datos (602301)	Sublime	
	Web Browser	
	Netbeans	OK
	JDK1.8	OK
	Adobe reader	
Teleinformática III (602001)	Nmap	OK
	Wireshark	
	Gedit	OK
	Openssh-server	
	Apache2	OK
	bash	OK
	vsftpd	
	pdf-viewer	
	net-tools	OK

Una vez validada la operación del sistema, se procedió a analizar la mitigación de riesgos que SASSI estaría en capacidad de realizar en un sistema convencional de prácticas de laboratorio, con los profesores y algunos estudiantes del curso, determinando lo siguiente:

RIESGO	**MECANISMO DE MITIGACIÓN**	**DESCRIPCIÓN**
Acceso abusivo a la sala. o suplantación	Lectura de la huella, envío por canal cifrado al servidor, validación en el servidor. Electroimán de 600 lbs solo es activado mediante SASSI.	Un usuario no puede ingresar sin autorización, ya que mediante la autenticación multifactor basada en biometría,
Deficiente trazabilidad de uso.	Transacciones definidas sobre la BD Postgres. Registro de históricos de Acceso y herramientas de software usadas.	Ante la necesidad de recurrir a históricos de uso e ingreso
Hurto de equipos y componentes.	Autenticación fuerte de dos factores (Password y Biometría de huella dactilar)	Quien Ingresa asume el inventario de la sala durante el periodo de tiempo que la usa.
No repudio		Futura implementación: asociar la Huella con el certificado digital
Registro de ingreso incompleto.	Validación automática de datos de ingreso en tiempo real	Los formatos manuales de registro suelen quedar mal diligenciados o incompletos, SASSI
Legal	Delitos informáticos y violación de la propiedad intelectual (Legalidad del software).	en la Ley 63 de 2000 (Legalización de software en Colombia) y Ley 1273 de 2009 (Protección de la Información y los datos)

Se verifica la carga correcta de la interfaz de inicio de sesión de SASSI, sobre la cual se efectúa la autenticación biométrica de huella dactilar de cada profesor.

Figura 8. Interfaz de selección de Inicio de sesión SASSI

Una vez efectuada la primera fase de la validación biométrica se prosigue con la segunda fase que consiste en solicitar la contraseña.

Figura 9. Primer Fase Autentificación superada - SASSI

Superada la segunda fase de la autenticación, el módulo de control de acceso expide el menú de software a usar y se da apertura de la puerta de la sala.

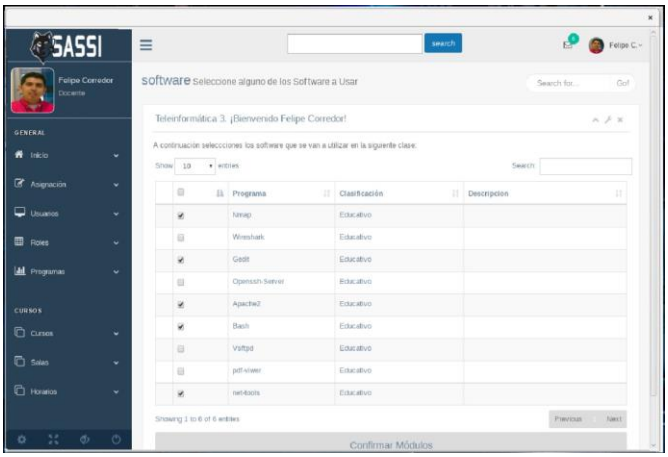

Figura 10. Interfaz de parametrización - SASSI

.

V. Conclusiones

Los servicios de autenticación y control de acceso no son excluyentes sino complementarios y deben integrarse con un adecuado manejador de sesiones y canales de comunicación cifrados. SASSI logró integrar estos servicios a través de la API de los lenguajes de programación JAVA y PHP, y demás componentes de hardware.

Estos servicios por si solos, se pueden implantar desde soluciones existentes en el mercado, pero actúan como elementos aislados, manejando sus propias fuentes de datos y con acceso restringido, son de difícil o nula capacidad de integración con otros sistemas y fuentes de datos.

El sistema desarrollado SASSI, planteó una alternativa de solución a la integración de estos servicios de seguridad en salas de cómputo en entornos académicos, los cuales se apoyan de sistemas de información y fuentes de datos que se comparten entre sí. El profesor como líder del proceso pedagógico, puede disponerlos para el análisis y toma de decisiones sobre su trabajo en el aula e incluso integrarlos a futuro con los datos almacenados en las plataformas virtuales como moodle.

Agradecimientos

Los autores expresan su gratitud a Dios y sus Familias, quienes siempre apoyaron este proceso. De igual manera, a la Universidad de los Llanos por creer en este Proyecto de investigación (“Código C05-F02-040-2016”) y financiarlo.

Referencias

[1] O. A. N, “Access Control Via Biometric Authentication System,” vol. 9, no. 4, pp. 54–64, 2011.

[2] S. Benziane and A. Benyettou, “An introduction to Biometrics,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 9, no. 4, pp. 40–47, 2011.

[3] “VIII Encuesta Latinoamericana de Seguridad de la Información Nuevos horizontes para América Latina Jeimy J. Cano M., Ph.D, CFE Gabriela María Saucedo Meza, MDOH,” 2016.

[4] Y. Mittal, A. Varshney, P. Aggarwal, K. Matani, and V. K. Mittal, “Fingerprint biometric based Access Control and Classroom Attendance Management System,” in 2015 Annual IEEE India Conference (INDICON), 2015, pp. 1–6.

[5] “VIII Encuesta Latinoamericana de Seguridad de la Información Nuevos horizontes para América Latina Jeimy J. Cano M., Ph.D, CFE Gabriela María Saucedo Meza, MDOH,” 2016.

[6] S. Kumari, X. Li, F. Wu, A. K. Das, K.-K. R. Choo, and J. Shen, “Design of a provably secure biometrics-based multi-cloud-server authentication scheme,” Futur. Gener. Comput. Syst., 2016..

[7] Oficina Asesora. de Planeación – Universidad de los Llanos, “Boletin estadistico Unilanos - 2015 - 2,” 2015.

[8] Trend Micro and Oea, “Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas,” 2015.

[9] E. Kennedy and C. Millard, “Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States,” Comput. Law Secur. Rev., vol. 32, no. 1, pp. 91–110, Feb. 2016.

[10] S. Mahnken, “Today’s authentication options: the need for adaptive multifactor authentication,” Biometric Technol. Today, vol. 2014, no. 7, pp. 8–10, Jul. 2014.

Felipe Andrés Corredor Magister en Software libre; en el área de administración de redes y sistemas operativos. Especialista en Soluciones telemáticas e Ingeniero de Sistemas. Certificado ISO27001, Investigador Junior (Colciencias), Docente de planta e investigador de la Escuela de ingeniería de la **Universidad de los Llanos**. Sus áreas de desempeño son la seguridad informática y los sistemas distribuidos. Lidera el Grupo de investigación en Tecnologías abiertas GITECX, reconocido por Colciencias.

Wolfang Sebastián Corredor En proceso de grado de Ingeniero de Sistemas por la **Universidad de los Llanos**, Actualmente es integrante activo del Grupo de Investigación GITECX. Sus áreas de desempeño son el desarrollo para móviles/web, desktop y la seguridad informática. Actualmente es Estudiante participante en Investigación en proyecto financiado por la Dirección General de Investigaciones..

Javier Eduardo Martínez Baquero Magister en Tecnología educativa; Especialista en Instrumentación Industrial. Docente de planta e investigador de la Escuela de ingeniería de la **Universidad de los Llanos**. Director de la Especialización en Instrumentación y control industrial. Sus áreas de desempeño son la Automatización, Instrumentación..