UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Diaz Bustamante, Wilson (orcid.org/0000-0002-4594-7594)

Muñoz Apagüeño, Vladik (orcid.org/0000-0003-3659-6371)

ASESORA:

Dra. Mescua Ampuero, Lizeth Erly (orcid.org/0000-0003-2748-479X)

LÍNEA DE INVESTIGACIÓN:

Sistemas Información y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

TARAPOTO – PERÚ

2023

Dedicatoria

A mis padres, quienes han sido mi faro en cada etapa de mi vida, su amor, sacrificio y apoyo incondicional han sido la fuerza impulsora detrás de cada logro. A mis amados hijos Stiven y Jade, quienes han sido mi fuente inagotable de inspiración y motivación. Su alegría y comprensión durante mis largas horas de dedicación a este proyecto han sido mi mayor impulso. A mi esposa J. Elizabeth, mi compañera incansable en este viaje, gracias por tu inquebrantable apoyo y comprensión, que han sido mi roca en cada desafío. A mis amigos y seres queridos, cuyo constante apoyo ha sido un regalo invaluable. A cada persona que ha dejado una huella en este camino, les dedico este trabajo con profundo agradecimiento y aprecio.

Wilson.

Este proyecto es un tributo a mi amada hija, cuya presencia ha sido mi faro en este viaje de descubrimiento y creación. Tu existencia me motiva a esforzarme más y a alcanzar nuevas metas. Este logro es un reflejo de tu luz en mi vida. Y a todos los que han jugado un papel importante en la realización de este proyecto, les estoy eternamente agradecido. Pero a ti, mi hija, te dedico este trabajo, como un pequeño reflejo de mi inmenso amor y orgullo por ti. Gracias.

Vladik.

Agradecimiento

En el camino de esta investigación, he sido bendecido con el apoyo y la guía de numerosas personas que han contribuido de manera invaluable a la culminación de este trabajo. Mi profundo agradecimiento se dirige en primer lugar a Dra. Mescua Ampuero, Lizeth Erly, cuya sabiduría, orientación y dedicación fueron fundamentales en cada etapa de este proceso. Agradezco sinceramente a mi familia por su inquebrantable aliento y comprensión durante los momentos desafiantes. También reconozco a mi compañero de tesis, por su colaboración y apoyo constante. Este logro no habría sido posible sin el respaldo de todas estas personas, y les estoy eternamente agradecido por su contribución a esta tesis.

Wilson & Vladik

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, LIZETH ERLY MESCUA AMPUERO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - TARAPOTO, asesor de Tesis titulada: "Sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023", cuyos autores son MUÑOZ APAGÜEÑO VLADIK, DIAZ BUSTAMANTE WILSON, constato que la investigación tiene un índice de similitud de 12.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

TARAPOTO, 23 de Noviembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
LIZETH ERLY MESCUA AMPUERO **DNI:** 42694079 **ORCID:** 0000-0003-2748-479X	Firmado electrónicamente por: MAMPUEROL8 el 23-12-2023 12:35:19

Código documento Trilce: TRI - 0663087

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Originalidad de los Autores

Nosotros, MUÑOZ APAGÜEÑO VLADIK, DIAZ BUSTAMANTE WILSON estudiantes de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - TARAPOTO, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. Hemos mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	**Firma**
VLADIK MUÑOZ APAGÜEÑO **DNI:** 44443927 **ORCID:** 0000-0003-3659-6371	Firmado electrónicamente por: MMUNOZAP el 23-11-2023 09:59:36
WILSON DIAZ BUSTAMANTE **DNI:** 43238538 **ORCID:** 0000-0002-4594-7594	Firmado electrónicamente por: DDIAZBU el 23-11-2023 22:40:08

Código documento Trilce: TRI - 0663077

INVESTIGA UCV

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

En este estudio de investigación se determinó, cómo el sistema de control biométrico incide en la gestión de accesos de empleados del Hospital MINSA – Moyobamba. Dicha investigación por su objetivo se clasificó como explicativa, adoptando un enfoque de naturaleza aplicada, y un diseño preexperimental. La población estuvo conformada por un total de 14 trabajadores, de los cuales 5 trabajadores pertenecen al área de Recursos Humanos y 9 trabajadores al área de TI. La muestra es censal; se utilizaron dos instrumentos: ficha de observación y un cuestionario.

Como resultados, se obtuvo un sig. de 0.001 el cual es inferior a 0.05, esto permite con un nivel de confianza del 95% afirmar que el sistema de control biométrico ejerce una incidencia positiva y significativa en la gestión de accesos de empleados de un Hospital Moyobamba, 2023.

En el capítulo I se redacta la introducción, posteriormente se aborda el marco teórico en el capítulo II, luego se plantea la metodología en el capítulo III, en el capítulo IV se muestran los resultados, después se lleva a cabo la discusión de los resultados en el capítulo V y finalmente en el capítulo VI se redacta las conclusiones.

Palabras clave: Gestión de accesos, sistema de control biométrico, biometría, seguridad

Abstract

In this research study, it was determined how the biometric control system affects the access management of employees of the MINSA Hospital - Moyobamba. Due to its objective, this research was classified as explanatory, adopting an applied nature approach, and a pre-experimental design. The population was made up of a total of 14 workers, of which 5 workers belong to the Human Resources area and 9 workers to the IT area. The sample is census; Two instruments were used: observation sheet and a questionnaire. As results, a sig. of 0.001 which is less than 0.05, this allows with a confidence level of 95% to affirm that the biometric control system has a positive and significant impact on the access management of employees of a Moyobamba Hospital, 2023.

In chapter I the introduction is written, then the theoretical framework is addressed in chapter II, then the methodology is presented in chapter III, in chapter IV the results are shown, then the discussion of the results is carried out in Chapter V and finally in Chapter VI the conclusions are drawn up.

Keywords: Access management, biometric control system, biometrics, security

I. INTRODUCCIÓN

En la actualidad, la gestión de accesos, así como la seguridad en los lugares de trabajo se han convertido en temas prioritarios en diversos sectores. En particular, los hospitales y centros de salud requieren de medidas efectivas para garantizar el control de ingreso de su personal, lo cual es fundamental para proteger la integridad de pacientes, empleados y visitantes. Es por ello que, en el año 2023, el Hospital MINSA de Moyobamba está en proceso de implementar un sistema de control biométrico que posibilite la gestión de accesos de sus empleados, para lo cual se utilizará tecnología de vanguardia de tal manera que permita asegurar una mayor eficiencia, garantizando seguridad en el acceso al recinto, al mismo tiempo que se optimiza la gestión de los registros tanto de entrada como de salida del personal.

La gestión de accesos a los empleados se ha vuelto cada vez más compleja debido a la gran cantidad de empleados y funciones que se realizan. Una de las tareas más importantes para una entidad es llevar un control de asistencia de los empleados, lo que a menudo resulta complicado y propenso a errores, es por ello que la gestión de accesos se posiciona como uno de los aspectos más cruciales e importantes para el desarrollo óptimo de una institución. En este sentido, el control de asistencia de los empleados es una tarea fundamental para garantizar la eficacia y efectividad del trabajo que cumple cada uno de los empleados.

Las formas de identificación del personal se han basado principalmente en el uso de carnets de entrada, uso de contraseñas o tokens, pero con el avance de la tecnología han ido mostrando cada vez mayores debilidades y son vulnerables con mayor facilidad, es por ello que la identificación biométrica sobresale como un método más eficiente y seguro para la identificación de personal.

La biometría, como tecnología de reconocimiento de patrones biológicos, ha sido ampliamente utilizada en todo el mundo en diferentes ámbitos, tales como la seguridad, la identificación personal, el control de acceso, la banca y la justicia, entre otros. Su uso se ha vuelto cada vez más común debido a su precisión y eficacia en la identificación de

personas.

La biometría se utiliza en diversas circunstancias de manera extensa, como en los aeropuertos, donde se utiliza para la identificación de pasajeros y empleados, en los sistemas de control de acceso a edificios gubernamentales, en la identificación de pacientes en hospitales y en la autenticación de usuarios en dispositivos móviles y computadoras. Además, la biometría ha adquirido un papel crucial en la batalla contra el crimen, ya que permite la identificación de criminales a través del reconocimiento de sus rasgos faciales, de sus huellas digitales o de su ADN.

En definitiva, la biometría ha llegado a ser considerada como una herramienta de seguridad imprescindible en una gran parte de las naciones alrededor del mundo, y se espera que su uso continúe creciendo en los próximos años debido a su eficacia y a la constante evolución tecnológica en este ámbito.

Se formuló como problema general ¿De qué manera el sistema de control biométrico incide en la gestión de accesos de empleados del Hospital MINSA – Moyobamba?, y como problemas específicos se formuló las siguientes preguntas: ¿De qué manera el sistema de control biométrico incide en la dimensión seguridad de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba?, ¿De qué manera el sistema de control biométrico incide en la dimensión privacidad de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba?, ¿De qué manera el sistema de control biométrico incide en la dimensión validación de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba?, ¿De qué manera el sistema de control biométrico incide en la dimensión eficiencia de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba?.

La investigación se justificó básicamente por las necesidades que tiene la organización, en este caso el Hospital MINSA de Moyobamba, debido a que el control de acceso se realizó aun de manera rudimentaria utilizando hojas de cálculo, y la sistematización de la gestión de accesos, mejora la seguridad, la privacidad, la validación de los activos del personal trabajador, pacientes y familiares que ingresan al recinto, generando

procesos más eficientes.

El objetivo general de esta investigación fue: determinar de qué manera el sistema de control biométrico incide en la gestión de accesos de empleados del Hospital MINSA – Moyobamba, y como objetivos específicos se formuló lo siguiente: determinar de qué manera el sistema de control biométrico incide en la dimensión seguridad de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba; determinar qué manera el sistema de control biométrico incide en la dimensión privacidad de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba; determinar de qué manera el sistema de control biométrico incide en la dimensión validación de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba; determinar de qué manera el sistema de control biométrico incide en la dimensión eficiencia de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba.

Como hipótesis general se planteó lo siguiente: El sistema de control biométrico incide de manera positiva en la gestión de accesos de empleados del Hospital MINSA – Moyobamba, y como hipótesis específicos se formuló lo siguiente: El sistema de control biométrico incide de manera positiva en la dimensión seguridad de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba; el sistema de control biométrico incide de manera positiva en la dimensión privacidad de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba; el sistema de control biométrico incide de manera positiva en la dimensión validación de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba; el sistema de control biométrico incide de manera positiva en la dimensión eficiencia de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba.

II. MARCO TEÓRICO

Como antecedentes internacionales respecto a los sistemas biométricos, se tiene:

(Rosado y Guaña 2018) en su artículo analizan y determinan las métricas definidas en los estándares ISO/IEC 9126-2 y 9126-3 orientadas a sistemas biométricos. Se detallan las características específicas de cada métrica con el propósito de alcanzar los resultados previstos. Estos resultados son evaluados mediante niveles de puntuación que reflejan el nivel de eficiencia de cada sub característica. Como resultado, se identificó una falta de eficiencia del 5% y un nivel de cumplimiento del 95%. Metodológicamente manifiestan que la norma ISO 9126 propone un modelo para la evaluación de la calidad tanto interna y como externa, el cual se divide en seis características: usabilidad, funcionalidad, fiabilidad, eficiencia, portabilidad y mantenibilidad. Cada una de estas características se subdivide en sub características que son sujetas a ser evaluadas mediante métricas internas o externas. Según los resultados obtenidos, las medidas estipuladas en los estándares ISO/IEC 9126-2 y 9126-3 son efectivas para realizar una evaluación adecuada de la característica de eficiencia. Además, se nota una correlación significativa entre la eficiencia y los atributos de los elementos de los aparatos utilizados en el sistema de computación.

Por otro lado (Reyes Parra y Verástegui Gonzáles 2018), en su artículo presentan la descripción del procedimiento utilizado para crear un modelo preliminar de sistema de información biométrica basado en huellas dactilares, el cual tiene como propósito administrar la admisión y el almacenamiento de información de los usuarios en la Universidad de la Amazonia. En tanto para la creación, se decidió emplear tecnologías que tienen código abierto que posibilitan realizar ajustes en el funcionamiento según los procedimientos y requisitos particulares de la institución universitaria. Entre estas tecnologías, se encuentra el sensor biométrico dactilar FMP10A, que permite hacer modificaciones en el protocolo de

manejo o procesamiento de datos biométricos. No obstante, la habilidad para recolectar imágenes de huellas dactilares está restringida, la capacidad de almacenamiento de su memoria flash permite guardar hasta 165 registros, limitando su utilización y su aplicación. En el marco de este trabajo se integraron funciones adicionales, que permiten la extracción, comunicación y validación de datos, este logro se alcanzó gracias a la centralización de los procesos.

Por su parte (Becerra et al. 2020), manifiestan que la identificación biométrica implica el procesamiento de características físicas y signos biológicos, y los sistemas de biometría son constantemente susceptibles a ataques, lo que requiere un desarrollo continuo para mantener la confianza en ellos. En su trabajo, se analizan las repercusiones de la calidad en la información de la identificación biométrica y se considera su importancia en los sistemas de gestión de accesos. Se plantea un enfoque de integración de datos para la creación de sistemas de biometría que tenga en cuenta la evaluación de la excelencia de los datos. Este modelo se basa en el modelo JDL (Joint Directors of Laboratories) de fusión de datos, que incluye el procesamiento de datos en bruto, la detección de patrones, la evaluación de la situación y el riesgo o impacto. Los resultados demuestran la funcionalidad del modelo propuesto y su potencial en comparación con otros enfoques de identificación convencionales, teniendo en cuenta la evaluación del riesgo.

También (Barka et al. 2022), en su artículo presentan la realizacion de un sistema de EHR en cadena de bloques (BBEHR) basado en datos biométricos, un prototipo que identifica de forma única a los pacientes, les permite controlar el acceso a sus EHR y garantiza el acceso recuperable a sus EHR. Este enfoque supera la dependencia del enfoque de clave privada/pública utilizado en gran medida por las tecnologías de cadena de bloques para identificar a los pacientes, lo que se vuelve más crucial en situaciones en las que la pérdida de la clave privada dificulta permanentemente la capacidad de acceder a los EHR de los pacientes. La solución planteada abarca la selección de componentes, la implementación

de alto nivel y la integración de subsistemas, así como la codificación de un prototipo para validar la mitigación del riesgo de pérdida permanente del acceso a los EHR mediante el uso de las huellas dactilares de los pacientes. Un análisis del rendimiento del BBEHR mostró la solidez y la eficacia de nuestro sistema a la hora de identificar a los pacientes y garantizar el control de acceso de sus EHR mediante el uso de contratos inteligentes basados en cadenas de bloques sin gastos adicionales.

Por su parte (Troshkov et al. 2021), manifiestan en su artículo que la base de datos actual de legislación y regulación de características biométricas para la seguridad de TI es insuficiente y tiene un sistema imperfecto. Las principales desventajas incluyen la falta de un sistema y una metodología para construir la identificación/autenticación biométrica que permita la administración del acceso o entrada a los recursos de información resguardados, conocimiento insuficiente de todas las posibles características biométricas de una persona, un modelo imperfecto del sistema biométrico y un enfoque estático para evaluar el control de acceso. En consecuencia, se da la necesidad de desarrollar un sistema biométrico de identificación/autenticación para restringir el acceso a los recursos de información en diferentes áreas.

En este sentido, proponen la sistematización del sistema biométrico de protección y administración del acceso a la información.

También (Dumitrescu 2019), en su artículo de investigación manifiesta que el reconocimiento facial es una habilidad crucial utilizada por los humanos en su vida cotidiana para identificar individuos. Aunque es una técnica robusta y no invasiva, representa un desafío en la disciplina de visión artificial y reconocimiento de diferentes tipos de patrones debido a la necesidad de detectar y reconocer un rostro en imágenes, independientemente de la iluminación, la expresión, la iluminación y la pose. Este artículo presenta un enfoque innovador para abordar problemas de representación del modelo facial y coincidencia en el reconocimiento facial. El enfoque se basa en la combinación de múltiples niveles de funcionalidades de Gabor y técnicas de Deep Learning. Los resultados

demostraron que este nuevo algoritmo de reconocimiento facial supera a los métodos convencionales, como el reconocimiento facial global Gabor basado en PCA, en términos de tasa de reconocimiento.

Respecto a la gestión de accesos, (Rasouli y Valmohammadi 2020), refieren que en los últimos años ha surgido un subgénero de la gestión tradicional de identidades y accesos (IAM) llamado administración de identidades y accesos de los clientes, el cual se enfoca en la conectividad con el cliente al acceder a cualquier tipo de sistemas, locales y en la nube, desde el registro hasta el seguimiento. El objetivo de dicho estudio es presentar diferentes dimensiones del CIAM para su aplicación en las organizaciones. Para recopilar los datos necesarios se realizó una investigación detallada de la literatura y una entrevista semiestructurada con seis expertos en IAM digital. Mediante técnicas de análisis de contenido se encontraron cuatro categorías importantes que afectan la identificación de las dimensiones del CIAM: gestión de identidad de los clientes, gestión de acceso de los clientes, tecnología de la información y gestión empresarial.

También (Rubenstein et al. 2020), dentro de documento científico tiene como objetivo identificar las prioridades para mejorar la organización sanitaria y la gestión del acceso de los pacientes a la atención primaria utilizando evidencia previa y la opinión de partes interesadas. Se llevó a cabo un análisis de partes interesadas utilizando Delphi modificado con panel anclado con una revisión sistemática. Se seleccionaron 20 panelistas que representaron a diferentes grupos de partes interesadas, incluyendo pacientes, proveedores, legisladores, compradores y pagadores de servicios de salud. Se aplicó una encuesta previa al panel que abordó más de 80 aspectos de la gestión de acceso a las organizaciones sanitarias, incluyendo la definición de gestión de acceso. Los panelistas discutieron las calificaciones basadas en encuestas durante una reunión en persona de dos días y volvieron a votar después. En un segundo panel, se centraron en cada prioridad final y desarrollaron recomendaciones y sugerencias para su implementación. El panel logró un consenso sobre las definiciones de

acceso óptimo y gestión de acceso, estableciendo 8 prioridades y de 1 a 3 recomendaciones por prioridad para orientar la gestión del acceso. Cada recomendación está respaldada por sugerencias de implementación referenciadas y aprobadas por el panel. Las prioridades abordan dos objetivos de la estructura organizacional, cuatro procesos de mejoras y dos resultados. Los objetivos de la estructura organizacional son liderazgo interdisciplinario del sitio de atención primaria, grupo claramente identificado y estructura de gestión de la práctica. Los procesos de mejora incluyen gestión de acceso telefónico de pacientes, personal de contingencia, enfermería gestión de la demanda a través de la coordinación de la atención y gestión proactiva de la demanda mediante la optimización de los horarios de visitas del proveedor. Los resultados incluyen la calidad de las experiencias de acceso de los pacientes y la moral del proveedor y del personal.

Como antecedentes nacionales se tiene: (Gastelo y Cabrera 2019), manifiestan que la Asociación Guadalupana no tiene un sistema de control de acceso efectivo que pueda identificar a los usuarios que ingresan a sus instalaciones, lo que ha causado problemas como robos, pérdida de información y suplantación de identidad. Para solucionar este problema, se realizó una investigación en la que se utilizaron herramientas tecnológicas como un lector de huellas dactilares y una plataforma web para diseñar un sistema de validación y autenticación biométrica dactilar que mejoraría el control de acceso en la Asociación Guadalupana. Los resultados indican que esta solución proporcionaría una mayor seguridad tanto para los trabajadores como para los asociados que ingresan a la asociación, lo que permitiría mitigar los problemas mencionados anteriormente.

También se tiene como antecedente a (Díaz y Flores 2019), quienes realizan su investigación en el seno de la destacada facultad de Ciencias Físicas y Matemáticas de la reconocida Universidad Nacional Pedro Ruiz Gallo que utilizaron fichas impresas para el registro de personal desde sus inicios, la organización no cuenta con una herramienta de seguimiento adecuada para la gestión de ingresos y salidas del personal, para

simplificar la tarea de gestionar las fechas de inasistencias y tardanzas. Para solucionar este problema, se utilizaron conceptos de biometría en microcontroladores, desarrollo de aplicaciones haciendo uso de los principios de programación orientada a objetos y sistemas de bases de datos. Se realizaron pruebas en campo en el lapso de 30 días, y aunque se encontraron problemas de conectividad, autenticación y diseño, se logró almacenar y trabajar con la data de registro y crear cuadros de exportación listos para imprimir. En conclusión, el prototipo demostró ser una solución efectiva que no genera retrasos, no requiere personal de supervisión y reduce la cantidad de papeleo.

Respecto a la variable sistema de control biométrico, se recurrió a la bibliografía, donde (Garrido Iglesias et al. 2017), manifiesta que en nuestra sociedad digital, las personas interactúan constantemente compartiendo información personal entre sí, lo que significa que ciertos datos personales serán necesariamente conocidos por terceros, es allí donde la biometría encaja en el modelo de comunicación para identificación y por medio de ello acceder a algún tipo de servicio, producto o a algún recinto de allí que se muestra mayor información de la variable de estudio biometría, es por ello que (Sánchez Calle 2005) define a la biometría informática como el campo que busca aplicar técnicas numéricas y de inteligencia artificial para lograr la autenticación e identificación de forma automática de individuos mediante un sistema de seguridad informática. Las técnicas biométricas se enfocan en medir y analizar uno o varios rasgos del individuo (ya sean estáticos o dinámicos) con el fin de reconocerlo o verificar su identidad automáticamente. La biometría estática se enfoca en medir rasgos anatómicos del usuario, como huellas digitales, imágenes faciales, geometría de la mano, patrones de iris y retina, entre otros. La biometría dinámica, por otro lado, se enfoca en medir características del comportamiento del usuario, como firma manuscrita, patrón de voz, gestos, cadencia del paso, entre otros.

Por otro lado, (Serratosa 2018), define a la biometría como la disciplina que se enfoca en la evaluación de las distancias y ubicaciones relativas entre las diversas partes del cuerpo humano con el objetivo de

reconocer y categorizar individuos. En la actualidad, existen varios rasgos biométricos que se utilizan para la identificación o clasificación de personas, como la cara, las huellas dactilares, la mano, la retina, el iris, o la firma. La biometría, y en particular el estudio de las huellas dactilares, se originó a finales del siglo XIX, cuando se utilizaba en actividades forenses para identificar a delincuentes o personas desconocidas.

Por otro lado se tiene a otros autores que defines a la biometría de la siguiente manera: Según (Rathgeb y Uhl 2019) define a la biometría como el reconocimiento automatizado de personas de acuerdo a sus características biológicas y de comportamiento; (Gniewek, Schreck y Hallatschek 2019), define a la biometría como el campo de estudio que involucra la medición y análisis de características biológicas o conductuales únicas de un individuo para su identificación y verificación; de acuerdo a (Preston y Ma 2018), definen la biometría como el uso de características biológicas o conductuales únicas para cada persona utilizadas para confirmar y verificar de su identidad. Por su parte (Minaee et al. 2019), La biometría es una técnica utilizada en la autenticación y verificación de las personas a través de características únicas e innatas, como la huella dactilar, la voz, el iris o la cara.

Actualmente, la biometría se emplea en diversas aplicaciones, desde el control de acceso en aeropuertos hasta la seguridad en instalaciones nucleares o militares, e incluso en la entrada a oficinas o piscinas municipales. Debido a la creciente presencia de la biometría en nuestras vidas cotidianas, es esencial que los profesionales informáticos e ingenieros estén familiarizados con los conceptos básicos de esta disciplina.

Según (Wayman, Jain, Maltoni y Malo, 2005), citado por (Huesca González 2021), manifiestan que los sistemas biométricos son sistemas automatizados que utilizan patrones para identificar o autenticar a una persona a través de sus características biométricas. Estos sistemas obtienen un conjunto de características a partir de los rasgos físicos de un individuo, los comparan con las características almacenadas en una base de datos y toman una decisión basada en el resultado de dicha comparación (Jain y Ross 2008)

El reconocimiento biométrico se basa en el uso de diversas características anatómicas (como las huellas dactilares, la cara o el iris) y de comportamiento (como la forma de hablar, la firma o la escritura en un teclado) que se conocen como identificadores o rasgos biométricos. Estos identificadores son utilizados para identificar a los individuos de manera automática. De acuerdo con el contexto de la aplicación biométrica, se diferencian dos tipos de sistemas; los sistemas de verificación, los cuales comparan la característica biométrica recién capturada con la que fue registrada previamente durante el proceso de inscripción, de esta manera, se verifica la identidad de la persona en consideración. Por otro lado, se cuentan con los sistemas de identificación, los cuales identifican a una persona mediante la búsqueda o consulta en base de datos de la característica biométrica que mejor coincida con la utilizada para su registro en el sistema. De esta forma, se logra el reconocimiento de la persona en cuestión (Serratosa 2018).

De acuerdo a («IBM Documentation» 2021) La identificación se refiere a la habilidad de distinguir a un usuario de manera única dentro de un sistema o aplicación en ejecución. La autenticación, por su parte, se relaciona con la capacidad de demostrar que el usuario o aplicación es verdaderamente quien afirma ser.

Los sistemas de verificación e identificación, necesitan de un proceso intermedio que es el sistema de matriculación, que es el encargado de recoger los rasgos biométricos, este proceso es muy importante porque relaciona la identificación con los rasgos biométricos de las personas.

A continuación, se presentan los esquemas que representan cada uno de los procesos:

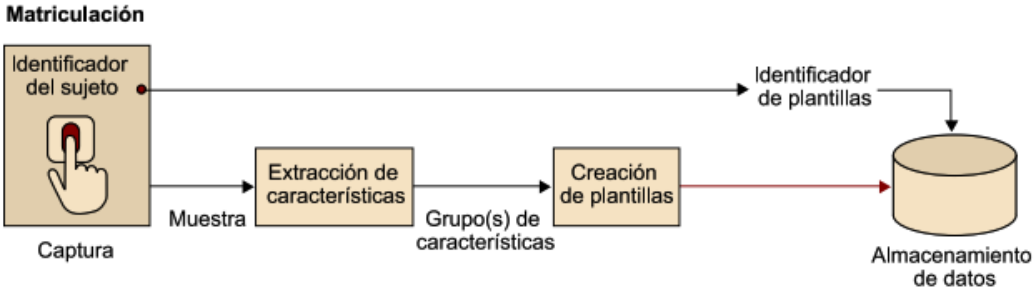


Figura 1. Proceso de matriculación

Fuente: Serratosa, 2018

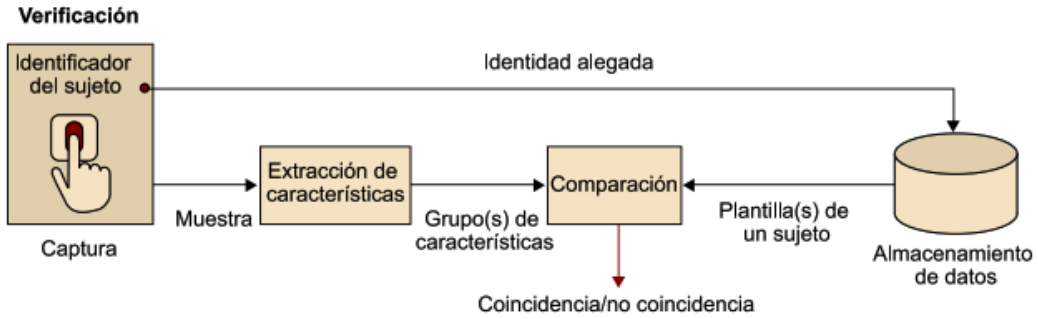


Figura 2. Proceso de verificación

Fuente: Serratosa, 2018

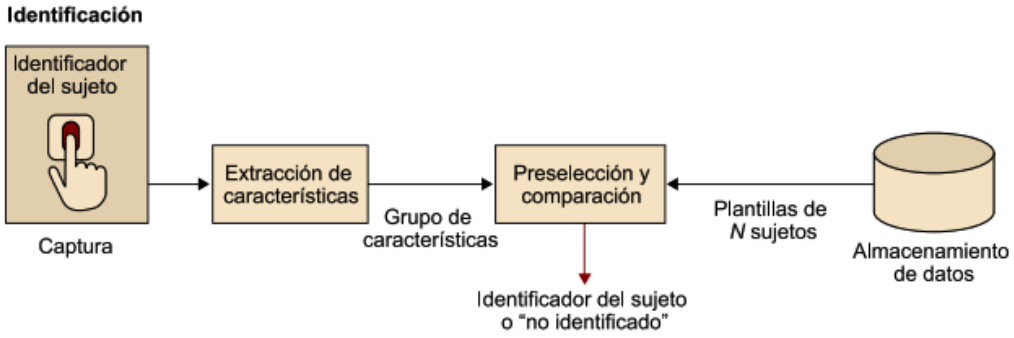


Figura 3. Proceso de identificación

Fuente: Serratosa, 2018

Según (Electronic_Identification 2021), la identificación electrónica es de muy importante en la satisfacción sobre las exigencias actuales que enfrentan las empresas y organizaciones en diversas campos o sectores. Aunque el término surgió originalmente gracias al avance tecnológico en el ámbito gubernamental, ha sido el sector privado el que ha asumido en liderar el desarrollo y uso de soluciones avanzadas y actualizadas de identificación electrónica. Cada proceso se rige por un conjunto especifico de normas y protocolos que definen detalladamente su funcionamiento y características. En el caso de la identificación electrónica, debido a su naturaleza y peculiaridades, es fundamental cumplir con normativas y estándares técnicos específicos para asegurar su correcto desarrollo.

Se pueden emplear tanto características anatómicas como de

comportamiento humano como identificadores biométricos para identificar o verificar individuos siempre y cuando cumplan con los siguientes requisitos: Particularidad, universalidad, medible, permanencia, adaptabilidad, rendimiento, no falsificable.

La biometría utiliza básicamente las siguientes características de las personas:

Huella dactilar: Es una representación de la epidermis del dedo que consta de un patrón de crestas y valles. Las crestas de los dedos permiten agarrar objetos y se forman mediante la combinación de influencias genéticos y ambientales. El código genético que está en nuestro ADN da instrucciones generales sobre la forma en que debe formarse la piel, pero la forma específica en que se forma es el resultado de eventos aleatorios. Por esta razón, incluso las huellas dactilares de gemelos idénticos son diferentes. Las huellas dactilares están completamente formadas alrededor de los siete meses de desarrollo del feto y no cambian a lo largo de la vida, excepto en casos de accidentes. Esta característica hace que las huellas dactilares sean un identificador biométrico muy atractivo para la identificación de personas (Maltoni y Cappelli 2018).

Reconocimiento facial: Hay una creciente necesidad de sistemas de reconocimiento facial robustos para ayudar en la batalla contra las fuerzas del crimen y el terrorismo, así como para proporcionar autenticación de usuario para mejorar la seguridad en espacios físicos y virtuales. Sin embargo, la identificación precisa de personas mediante una imagen de su cara y la comparación con bases de datos de rostros conocidos sigue siendo un problema desafiante debido a la variabilidad en las condiciones operativas y del entorno, como la iluminación, las rotaciones, las expresiones, el ángulo de la cámara, el envejecimiento, el maquillaje y los anteojos. Esta variabilidad afecta significativamente el rendimiento de los sistemas de reconocimiento facial, especialmente cuando se utilizan con grandes bases de datos. Por lo tanto, aunque se han implementado muchos sistemas de reconocimiento facial, su uso y precisión se limitan a escenarios operativos específicos debido a los errores de la tasa de aceptación falsa (FAR), de la misma manera sucede con la tasa de rechazo falso (FRR), que se consideran un problema importante. La FAR se refiere

a la probabilidad de que los sistemas acepten a una persona no autorizada, mientras que la FRR se refiere a la probabilidad de que los sistemas rechacen a una persona autorizada de manera incorrecta (Savvides, Heo y Park 2018).

Reconocimiento de iris: Durante los últimos 15 años, el campo del reconocimiento del iris ha experimentado un rápido desarrollo, pasando de ser una tecnología emergente con pocas demostraciones y patentes iniciales a convertirse en un campo convencional de la biometría con muchos investigadores activos en la industria y la academia. Actualmente, hay alrededor de 50 millones de personas inscritas en sistemas de reconocimiento de iris en todo el mundo. Sin embargo, otros sistemas también están siendo desarrollados, probados y demostrados en competencias patrocinadas por el gobierno, mostrando buenos resultados. En perspectiva futura es factible que exista una variedad de métodos y productos viables y quizás incluso interoperables disponibles para su implementación. Es importante tener en cuenta que el reconocimiento del iris está diseñado para su uso en modo de identificación, lo que significa que no se le pide al usuario que afirme su identidad, a diferencia de la simple verificación donde se realiza una prueba "uno a uno" (Daugman 2018).

Reconocimiento de geometría de la mano: Hand Geometry es una tecnología de autenticación que ha sido utilizada durante mucho tiempo. Se cree que las huellas de manos encontradas en pinturas antiguas en la caverna Chauvet, datadas en 31.000 años mediante la técnica de carbono, podrían haber sido la firma única del artista y representan uno de los primeros usos conocidos de la Hand Geometry para la identificación. Pero este no fue su último uso. En el año 1858, Sir William Herschel pidió a Rajyadhar Konai, un hombre de negocios local, que imprimiera su mano en el reverso de un contrato para vincular de manera única a Konai con el contrato. Este fue el inicio de la primera captura sistemática registrada de imágenes de manos y dedos con fines de identificación. En los años 70, Identimation introdujo Identimat, el primer escáner comercial Hand Geometry, utilizando alrededor de 1000 vatios para activar fotocélulas escaneadas mecánicamente (Sidlauskas y Tamer 2018).

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

Tipo de investigación

El enfoque de investigación utilizado fue de naturaleza aplicada, orientada al enfoque cuantitativo, con el propósito de examinar un fenómeno y ampliar el conocimiento. Los resultados obtenidos nos permitieron abordar problemas y adoptar medidas prácticas relacionadas con la realidad que se ha estudiado (Concytec, 2018).

Diseño de investigación

La estructura del estudio fue pre-experimental, dado que sólo se realizó la manipulación de una de las variables, en este caso fue la variable dependiente gestión de accesos, puesto que se analizó la incidencia en un único momento. Fue de tipo longitudinal, porque se recopiló los datos en dos instancias de tiempo, un pre test y un post test. (Hernández y Mendoza 2018).

La representación visual se exhibe a través del siguiente gráfico:

Figura 4. Diseño de investigación

Donde:

G: Grupo

M_1: Grupo con pre-test

x: Sistema de control biométrico

M_2: Grupo post-test

3.2 Variables y operacionalización

- **Sistema de control biométrico**

  - **Definición conceptual**

    Los sistemas de control biométrico son sistemas automatizados que utilizan patrones para identificar o autenticar a una persona a través de sus características biométricas. (Wayman et al. 2019)

  - **Definición operacional**

    El sistema de control biométrico, será medido en función de las pruebas de funcionalidad de software, medidas en tiempo (minutos)

- **Gestión de accesos**

  - **Definición conceptual**

    La gestión de accesos se refiere al conjunto de procesos y herramientas que se utilizan para controlar y administrar el acceso a sistemas y recursos informáticos, como aplicaciones, bases de datos, archivos y redes, por parte de usuarios y grupos autorizados. (Villalón Millán, J.M)

    - **Definición operacional**

      La variable gestión de accesos se medirá mediante las dimensiones seguridad, privacidad, validación y eficiencia

3.3 Población, muestra, muestreo y unidad de análisis

Población

Nuestra población está compuesta por 5 trabajadores que laboran en el área de Recursos Humanos y 9 trabajadores del área de TI, que laboran en el Hospital MINSA – Moyobamba.

- **Criterio de inclusión**

Trabajadores que vienen laborando en los últimos 3 meses, tomando como referencia de inicio el mes de mayo del 2023, así

mismo a todos los trabajadores que tengan conocimiento sobre biometría y gestión de accesos.

- **Criterios de exclusión**

  Trabajadores sin conocimiento básico sobre biometría y gestión de accesos.

Muestra

La muestra consta de 14 trabajadores y fue censal, ya que fue necesario que cada uno de los trabajadores que cumplieron los requisitos de criterio de inclusión, estén registrados para poder identificarse al ingresar, durante y al salir del trabajo.

Muestreo

No se presenta algún tipo de muestreo, dado que la totalidad de la población fue considerada como muestra para este estudio.

Unidad de análisis

Cada uno de los trabajadores del Hospital MINSA – Moyobamba, que participó de la investigación y que cumple con el criterio de inclusión.

3.4 Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

La técnica aplicada para analizar, fue la observación la cual se aplicó a la variable sistema de control biométrico y la encuesta, que fue aplicada a la variable gestión de accesos.

Instrumentos de recolección de datos

Se utilizó una guía de observación conformada por 14 ítems y un cuestionario conformado por 17 ítems, el cual está estructurado

mediante la escala tipo Likert, la cual permitió medir cualitativamente a las variables de estudio y establecer su impacto de una variable sobre la otra.

Resumiendo, en una tabla la técnica e instrumento utilizado en esta investigación:

Tabla 1. Técnicas e instrumentos de recolección de datos

Instrumento	Técnica	Fuente informante
Ficha de observación	Observación	Sistema informático
Cuestionario	Encuesta	Empleados de Hospital Moyobamba

Fuente: Elaboración propia

Validez

La validez del instrumento se realizó por 3 profesionales expertos en ingeniería de sistemas, los cuales se encargaron de revisar el instrumento desde la perspectiva de suficiencia, claridad coherencia y relevancia.

Tabla 2. Listado de expertos

Experto	Especialidad
Mg. Miguel Ángel Román Martínez García	Ing. de Sistemas
Mg. Jaime Paolo Ramírez Meléndez	Ing. de Sistemas
Mg. Nixon Omar Fernández Carrión	Ing. de Sistemas

Nota. Mg.: Magíster; Dr.: Doctor

Confiabilidad

Para la obtención de la confiabilidad, se utilizó una prueba piloto de 10 trabajadores, a cuyas encuestas se les aplicó el coeficiente de Alfa de Cronbach el cual permitió medir la consistencia, la variabilidad total y homogeneidad de la encuesta.

Tabla 3. Alfa de Cronbach aplicada a la encuesta: Sistema de control biométrico para la gestión de accesos de empleados del Hospital MINSA – Moyobamba, 2023

Alfa de Cronbach	N° de elementos
0,759	10

Fuente: Elaboración propia

3.5 Procedimientos

Para el estudio se inició enviando una solicitud al director del Hospital MINSA – Moyobamba, para que brinde el permiso necesario, luego de haberse aprobado el permiso para el desarrollo del estudio se aplicó el cuestionario piloto a 14 trabajadores. En la siguiente fase del proyecto, que se enfocó en el desarrollo, se emplearon los instrumentos adecuados en función del tamaño de la población y muestra definida. Luego se realizó el análisis de los datos y se llegó a las conclusiones, contrastando la discusión con los antecedentes.

3.6 Método de análisis de datos

En el presente estudio, se empleó el software SPSS versión 27 en conjunto con las hojas de cálculo de Microsoft Excel para realizar el análisis de datos. Estas herramientas se utilizaron para obtener las tablas de distribución de frecuencias requerida en el análisis descriptivo. En cuento a la fase de análisis inferencial, se aplicó la prueba de normalidad de Shapiro-Wilk, considerando que la muestra consta de 14 trabajadores. Además, se utilizó la

prueba de Wilcoxon con el propósito de evaluar el impacto del sistema de control biométrico en la gestión de accesos.

3.7 Aspectos éticos

Para el desarrollo de la investigación se consideraron directrices éticas y los comportamientos aceptables en el ámbito de la investigación, se aplicaron las normas ISO-690 para las citas, que incluyen el nombre del autor y el año de la publicación al describir la problemática, los antecedentes y el marco teórico. Además, se respetó la normativa establecida de la Universidad César Vallejo y se aseguró la confiabilidad de los datos de los encuestados.

También se respetaron los siguientes principios del código de ética en la investigación: Destacando especialmente el principio de honestidad, porque se aseguró que los resultados sean transparentes, veraces y precisos, evitando el plagio; el principio de confidencialidad, protegiendo los datos de los participantes e información sensible; el consentimiento informado, el cual se realizó previamente a su inclusión en la muestra de estudio, el principio de equidad, para garantizar la igualdad de oportunidades en su participación en la investigación, sin discriminación alguna y el uso responsable de los resultados evitando su tergiversación e interpretación errónea.

IV. RESULTADOS

4.1 Estadísticas descriptivas del pretest y postest

Tabla 4. Medidas Descriptivas de Nivel de seguridad del sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023

Nivel	Pre test		Pos test	
	fi	hi%	fi	hi%
Muy bajo	2	14.3	0	0.0
Bajo	10	71.4	0	0.0
Regular	2	14.3	5	35.7
Bueno	0	0.0	6	42.9
Muy bueno	0	0.0	3	21.4
Total	14	100.0	14	100.0

Fuente: Elaboración propia, con datos de encuesta pretest y postest

Interpretación: De los 14 trabajadores del área de recursos humanos y del área de TI, del Hospital Moyobamba que fueron encuestados antes de implementar el sistema de control biométrico, el 14.3% manifiesta que el nivel de seguridad en la institución es muy bajo, el 71.4% responde que es bajo, y el 14.3% sostiene que es regular. Luego de haberse implementado el sistema de control biométrico, el 35.7% manifiesta que el nivel de seguridad en la institución es regular, el 42,9% responde que es bueno, y el 21.4% sostiene que es muy bueno. A nivel descriptivo se muestra una mejora pronunciada en la dimensión nivel de seguridad.

Tabla 5. Nivel de privacidad del sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023

Nivel	Pre test		Pos test	
	fi	hi%	fi	hi%
Muy bajo	1	7.1	0	0.0
Bajo	12	85.7	0	0.0
Regular	1	7.1	3	21.4
Bueno	0	0.0	9	64.3
Muy bueno	0	0.0	2	14.3
Total	14	100.0	14	100.0

Fuente: Elaboración propia, con datos de encuesta pretest y postest

Interpretación: De los 14 trabajadores del área de recursos humanos y del área de TI, del Hospital Moyobamba que fueron encuestados antes de implementar el sistema de control biométrico, el 7.1% manifiesta que el nivel de privacidad en la institución es muy bajo, el 85.7% responde que es bajo, y el 7.1% sostiene que es regular. Luego de haberse implementado el sistema de control biométrico, el 21.4% manifiesta que el nivel de privacidad en la institución es regular, el 64.3% responde que es bueno, y el 14.3% sostiene que es muy bueno. A nivel descriptivo se muestra una mejora pronunciada en la dimensión nivel de privacidad.

Tabla 6. Nivel de validación del sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023

Nivel	Pre test		Pos test	
	fi	hi%	fi	hi%
Muy bajo	5	35.7		0.0
Bajo	7	50.0		0.0
Regular	2	14.3	3	21.4
Bueno	0	0.0	4	28.6
Muy bueno	0	0.0	7	50.0
Total	14	100.0	14	100.0

Fuente: Elaboración propia, con datos de encuesta pretest y postest

Interpretación: De los 14 trabajadores del área de recursos humanos y del área de TI, del Hospital Moyobamba que fueron encuestados antes de implementar el sistema de control biométrico, el 35.7% manifiesta que el nivel de validación en la institución es muy bajo, el 50% responde que es bajo, y el 14.3% sostiene que es regular. Luego de haberse implementado el sistema de control biométrico, el 21.4% manifiesta que el nivel de validación en la institución es regular, el 28.6% responde que es bueno, y el 50% sostiene que es muy bueno. A nivel descriptivo se muestra una mejora pronunciada en la dimensión nivel de validación.

Tabla 7. Nivel de eficiencia del sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023

Nivel	Pre test		Pos test	
	fi	hi%	fi	hi%
Muy bajo	5	35.7	0	0.0
Bajo	8	57.1	0	0.0
Regular	1	7.1	8	57.1
Bueno	0	0.0	6	42.9
Muy bueno	0	0.0	0	0.0
Total	14	100.0	14	100.0

Fuente: Elaboración propia, con datos de encuesta pretest y postest

Interpretación: De los 14 trabajadores del área de recursos humanos y del área de TI, del Hospital Moyobamba que fueron encuestados antes de implementar el sistema de control biométrico, el 35.7% manifiesta que el nivel de eficiencia en la institución es muy bajo, el 57.1% responde que es bajo, y el 7.1% sostiene que es regular. Luego de haberse implementado el sistema de control biométrico, el 57.1% manifiesta que el nivel de eficiencia en la institución es regular, y el 42,9% responde que es bueno. A nivel descriptivo se muestra una mejora pronunciada en la dimensión nivel de eficiencia.

Tabla 8. Nivel de gestión de accesos de empleados de un Hospital Moyobamba, 2023

Nivel	Pre test		Pos test	
	fi	hi%	fi	hi%
Muy bajo	2	14.3	0	0.0
Bajo	12	85.7	0	0.0
Regular	0	0.0	3	21.4
Bueno	0	0.0	10	71.4
Muy bueno	0	0.0	1	7.1
Total	14	100.0	14	100.0

Fuente: Elaboración propia, con datos de encuesta pretest y postest.

Interpretación: De los 14 trabajadores del área de recursos humanos y del área de TI, del Hospital Moyobamba que fueron encuestados antes de implementar el sistema de control biométrico, el 14.3% manifiesta que la variable gestión de accesos en la institución es muy bajo, y el 85.7% responde que es bajo. Luego de haberse implementado el sistema de control biométrico, el 21.4% manifiesta que la variable gestión de accesos en la institución es regular, el 71.4% responde

que es bueno y el 7.1% sostiene que es muy bueno. A nivel descriptivo se muestra una mejora pronunciada en la variable gestión de accesos.

ANÁLISIS INFERENCIAL

4.2 Estadísticas inferenciales

Prueba de hipótesis

- **Prueba de hipótesis general**

H_0: El sistema de control biométrico no incide de forma significativa y positiva en la gestión de accesos de empleados del Hospital MINSA – Moyobamba

H_a: El sistema de control biométrico incide de forma significativa y positiva en la gestión de accesos de empleados del Hospital MINSA – Moyobamba

Tabla 9. Prueba de hipótesis general

Estadísticos de prueba[a]

	Gestión de accesos - Postest / Gestión de accesos - Pretest
Z	-3,296[b]
Sig. asintótica(bilateral)	**0,001**

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia, con datos de encuesta pretest y postest.

Interpretación: Según la prueba de hipótesis no paramétrica para variables cualitativas, se obtuvo un sig. de 0.001 menor a 0.05, lo cual permite afirmar con un 95% de confianza que el sistema de control biométrico incide de forma positiva y significativa en la gestión de accesos de empleados de un Hospital Moyobamba, 2023.

- **Prueba de hipótesis específica 1**

H_0: El sistema de control biométrico no incide de manera positiva en la dimensión seguridad de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba

H_a: El sistema de control biométrico incide de manera positiva en la dimensión seguridad de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba

Tabla 10. Prueba de hipótesis específica 1

Estadísticos de prueba[a]

	Nivel de seguridad - Postest - Nivel de seguridad - Pretest
Z	-3,327[b]
Sig. asintótica(bilateral)	**0,001**

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia, con datos de encuesta pretest y postest

Interpretación: Según la prueba de hipótesis no paramétrica para variables cualitativas, se obtuvo un sig. de 0.001 menor a 0.05, lo cual permite afirmar con un 95% de confianza que el sistema de control biométrico, incide de forma positiva y significativa en la dimensión nivel de seguridad de la gestión de accesos de empleados de un Hospital Moyobamba, 2023.

- **Prueba de hipótesis específica 2**

H_0: El sistema de control biométrico no incide de manera positiva en la dimensión privacidad de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba

H_a: El sistema de control biométrico incide de manera positiva en la dimensión privacidad de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba

Tabla 11. Prueba de hipótesis específica 2

Estadísticos de prueba[a]

	Nivel de privacidad - Postest - Nivel de privacidad - Pretest
Z	-3,304[b]
Sig. asintótica(bilateral)	**0,001**

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia, con datos de encuesta pretest y postest

Interpretación: Según la prueba de hipótesis no paramétrica para variables cualitativas, se obtuvo un sig. de 0.001 menor a 0.05, lo cual permite afirmar con un 95% de confianza que el sistema de control biométrico, incide de forma positiva y significativa en la dimensión nivel de privacidad de la gestión de accesos de empleados de un Hospital Moyobamba, 2023.

- **Prueba de hipótesis específica 3**

H_0: El sistema de control biométrico no incide de manera positiva en la dimensión validación de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba

H_a: El sistema de control biométrico incide de manera positiva en la dimensión validación de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba

Tabla 12. Prueba de hipótesis específica 3

Estadísticos de prueba[a]

	Nivel de validación - Postest - Nivel de validación - Pretest
Z	-3,301[b]
Sig. asintótica(bilateral)	**0,001**

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia, con datos de encuesta pretest y postest

Interpretación: Según la prueba de hipótesis no paramétrica para variables cualitativas, se obtuvo un sig. de 0.001 menor a 0.05, lo cual permite afirmar con un 95% de confianza que el sistema de control biométrico, incide de forma positiva y significativa en la dimensión nivel de validación de la gestión de accesos de empleados de un Hospital Moyobamba, 2023.

- **Prueba de hipótesis específica 4**

H_0: El sistema de control biométrico no incide de manera positiva en la dimensión eficiencia de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba

H_a: El sistema de control biométrico incide de manera positiva en la dimensión eficiencia de la variable gestión de accesos de empleados del Hospital MINSA – Moyobamba

Tabla 13. Prueba de hipótesis específica 4

Estadísticos de prueba[a]

	Nivel de eficiencia - Postest - Nivel de eficiencia - Pretest
Z	-3,303[b]
Sig. asintótica(bilateral)	**0,001**

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia, con datos de encuesta pretest y postest

Interpretación: Según la prueba de hipótesis no paramétrica para variables cualitativas, se obtuvo un sig. de 0.001 menor a 0.05, lo cual permite afirmar con un 95% de confianza que el sistema de control biométrico, incide de forma positiva y significativa en la dimensión nivel de eficiencia de la gestión de accesos de empleados de un Hospital Moyobamba, 2023.

V. DISCUSIÓN DE RESULTADOS

Basándonos en los resultados obtenidos en esta investigación, rechazamos la hipótesis nula general, la cual evidencia que el sistema de control biométrico incide de forma significativa y positiva en la gestión de accesos de empleados del Hospital MINSA – Moyobamba.

Con respecto a la dimensión nivel de seguridad, los resultados de esta investigación guardan relación con los obtenidos por Gastelo y Cabrera 2019, quienes luego de identificar problemas de robo, pérdida de información y suplantación de identidad, implementan una solución que proporcionó mayor seguridad tanto para los trabajadores como para los asociados que ingresan a la asociación, lo que permitió mitigar los problemas mencionados anteriormente. Esto demuestra la gran importancia que tiene hoy en día la seguridad informática, dado que, con el avance de las tecnologías y el crecimiento de la informatización, cada vez más se tiene dependencia de los medios digitales. Por otro lado, Díaz y Flores 2019, realizaron pruebas en campo, y aunque encontraron problemas de conectividad, autenticación y diseño, se logró almacenar y trabajar con la data de registro y crear cuadros de exportación listos para imprimir, concluyendo que el prototipo demostró ser una solución efectiva que no genera retrasos, no requiere personal de supervisión y reduce la cantidad de papeleo, mejorando los niveles de seguridad en la organización. Esta solución adiciona la funcionalidad de funcionar offline cuando existan inconvenientes en la red, y se sustenta bajo el principio de la disponibilidad, el cual es uno de los pilares en la seguridad informática

Respecto a la dimensión privacidad, existe coincidencias con Troshkov et al. 2021, quienes manifiestan que la falta de un sistema y una metodología para construir la identificación/autenticación biométrica que permita la administración, el acceso o entrada a los recursos de información protegidos. En consecuencia, implementan y mejoran los niveles de seguridad, mediante un sistema biométrico de identificación/autenticación para restringir el acceso a los recursos de

información en diferentes áreas. Esto demuestra que aunque dichas tecnologías existen desde hace ya muchos años, siguen evolucionando, bajo perspectivas diversas y con nuevos protocolos de seguridad, por ello dicha tecnología biométrica sigue siendo fundamental y de amplio uso en las organizaciones.

Tomando como referencia la dimensión nivel de validación, los resultados obtenidos en este estudio coinciden con los obtenidos por Barka et al. 2022, en su enfoque supera la dependencia del enfoque de clave privada/pública utilizado en gran medida por las tecnologías de cadena de bloques para identificar a los pacientes, lo que se vuelve más crucial en situaciones en las que la pérdida de la clave privada dificulta permanentemente la capacidad de acceder a los EHR de los pacientes. En su análisis del rendimiento del BBEHR mostró la solidez y la eficacia de su sistema a la hora de identificar a los pacientes y garantizar el control de acceso de sus EHR mediante el uso de contratos inteligentes basados en cadenas de bloques sin gastos adicionales, mostrando un buen nivel de validación. Esto demuestra la importancia de la validación en los sistemas de seguridad, así como de los algoritmos de encriptación utilizados para dicha función. También Reyes y Verástegui 2018, presentan la descripción del procedimiento utilizado para crear un modelo de sistema de información biométrico dactilar, el cual tiene como propósito administrar la admisión y el almacenamiento de información de los usuarios en la Universidad de la Amazonia, en su trabajo añadieron funciones adicionales, que permiten la extracción, comunicación y validación de datos gracias a la centralización de los procesos, demostrando su valía, mejorando un proceso relacionado a la seguridad en la entidad. Esto demuestra que cada vez más los procesos son centralizados en servidores, los cuales a su vez son configurados para cumplir tareas específicas y den soporte a los diferentes tipos de implementación de seguridad en las organizaciones.

Respecto al nivel de eficiencia, estos resultados coinciden con Rosado y Guaña 2018, quien en sus resultados evalúa mediante niveles de puntuación que reflejan el nivel de eficiencia de cada sub característica. Como resultado, se identificó una falta de eficiencia del 5% y un nivel de

cumplimiento del 95%. Asimismo, se observa una fuerte correlación entre la eficiencia y las características de los elementos de los dispositivos empleados en el sistema informático. Medir la eficiencia es fundamental, si no se mide no se sabe cómo estamos, por ello la importancia de adicionar a los procesos de seguridad, la medición de su eficiencia. También existen coincidencias con Dumitrescu 2019, quien basa su enfoque en la combinación de múltiples niveles de funcionalidades de Gabor y técnicas de Deep Learning. Los resultados demostraron que este nuevo algoritmo de reconocimiento facial supera a los métodos convencionales, como el reconocimiento facial global Gabor basado en PCA, en términos de tasa de reconocimiento, demostrando su eficiencia frente a otros modelos implementados, que no usan la inteligencia artificial. En este caso el autor complementa los niveles de seguridad con la inteligencia artificial, elemento fundamental ya que es una disciplina que está creciendo a pasos agigantados y cada día nos sorprende realizando actividades que en su momento solo lo hacían los humanos. Por otro lado, Becerra et al. 2020, en su trabajo, analizan las repercusiones de la calidad y eficiencia en la información de la identificación biométrica y se considera su importancia en los sistemas de gestión de accesos, para ello plantean un enfoque de integración de datos para la creación de sistemas de biometría que tenga en cuenta la evaluación de la excelencia de la información. Los resultados demuestran la funcionalidad y eficiencia del modelo propuesto y su potencial en comparación con otros enfoques de identificación convencionales, teniendo en cuenta la evaluación del riesgo. Al igual que Dumitrescu, pone énfasis en medir la eficiencia de la tecnología aplicada apara la seguridad, agregando la gestión del riesgo, que es fundamental en un sistema de seguridad.

En cuanto a la variable gestión de accesos Rubenstein et al. 2020, más que coincidencias o discrepancias, existe un modelo de buenas prácticas para ser aplicado, ya que abordan el problema realizando un análisis más riguroso y por consiguiente los resultados son más eficientes y certeros. Ellos han identificado las prioridades para mejorar la organización sanitaria y la gestión del acceso de los pacientes a la

atención primaria utilizando evidencia previa y la opinión de partes interesadas, para lo cual utilizaron el método Delphi modificado, el cual fue aplicado mediante una encuesta previa al panel que abordó más de 80 aspectos de la gestión de acceso a las organizaciones sanitarias, que luego de varios debates solo eligieron algunos aspectos donde destaca la gestión de accesos.

Es importante destacar que para mejorar los niveles de seguridad en las organizaciones, no solo pasa por elaborar software, o adquirir tecnologías relacionadas con el hardware, sino que es importante gestionar la seguridad de la información, dado que el eslabón más débil en los activos de información es el humano; además es importante recalcar que medir cada uno de los procesos de forma permanente y continuar con ellos, modificarlos o cambiarlos debe ser un proceso repetitivo como lo demuestra el ciclo de Demming.

VI. CONCLUSIONES

1. Se logró determinar con un 95% de confianza que el sistema de control biométrico incide de forma positiva y significativa en la dimensión nivel de seguridad de la gestión de accesos de empleados de un Hospital Moyobamba, 2023, ya que se evidenciaron mejoras en la seguridad del procesamiento, almacenamiento, integridad y confidencialidad. Los mayores cambios ocurren del 71.4% de nivel de seguridad bajo al 42.9% del nivel de seguridad bueno.
2. Se logró determinar con un 95% de confianza que el sistema de control biométrico incide de forma positiva y significativa en la dimensión nivel de privacidad de la gestión de accesos de empleados de un Hospital Moyobamba, 2023, ya que se evidenciaron mejoras en la protección, cifrado, retención, eliminación y monitoreo de los datos. Los mayores cambios ocurren del 85.7% de nivel de privacidad bajo al 64.3% del nivel de privacidad bueno.
3. Se logró determinar con un 95% de confianza que el sistema de control biométrico incide de forma positiva y significativa en la dimensión nivel de validación de la gestión de accesos de empleados de un Hospital Moyobamba, 2023, ya que se evidenciaron mejoras en la validación de accesos, precisión de los datos, identidades falsas, además de la validación por fechas y turnos. Los mayores cambios ocurren del 50% de nivel de validación bajo al 64.3% del nivel de validación bueno.
4. Se logró determinar con un 95% de confianza que el sistema de control biométrico incide de forma positiva y significativa en la dimensión nivel de eficiencia de la gestión de accesos de empleados de un Hospital Moyobamba, 2023, ya que se evidenciaron mejoras en el monitoreo, retrasos innecesarios, accesos y facilidad de uso. Los mayores cambios ocurren del 57.1% de nivel de eficiencia bajo al 57.1% del nivel de eficiencia regular.

VII. RECOMENDACIONES

Se recomienda que el Hospital Moyobamba continúe utilizando y fortaleciendo el sistema de control biométrico como un componente integral de su estrategia o plan de seguridad. Además, se sugiere que se realicen estudios adicionales para evaluar otros aspectos de la implementación y el impacto del sistema, lo que podría proporcionar información adicional sobre cómo optimizar su eficacia.

Se recomienda que el Hospital Moyobamba diseñar e implementar políticas sobre niveles de cifrado de datos y gestione de forma más eficiente los datos de extrabajadores, que ya no deben estar activos ni disponibles para consultas no autorizadas.

Dado que la validación precisa de accesos es crucial para garantizar la autenticidad y legitimidad de las interacciones en el entorno hospitalario, estos resultados tienen importantes implicaciones en el nivel de accesos, precisión de datos, e identificaciones falsas.

Se recomienda seguir mejorando los indicadores de eficiencia en el monitoreo, rapidez de acceso y facilidad de uso, dado que a la fecha aún existen algunas observaciones en la manipulación de información en tiempo real.

REFERENCIAS

BARKA, E., BAQARI, M.A., KERRACHE, C.A. y HERRERA-TAPIA, J., 2022. Implementation of a Biometric-Based Blockchain System for Preserving Privacy, Security, and Access Control in Healthcare Records. *Journal of Sensor and Actuator Networks* [en línea], vol. 11, no. 4, [consulta: 28 abril 2023]. DOI 10.3390/jsan11040085. Disponible en: https://www.proquest.com/docview/2756736420/abstract/80A44624AF614B19PQ/1.

BECERRA, M.A., LASSO-ARCINIEGAS, L., VIVEROS, A., SERNA-GUARÍN, L., PELUFFO-ORDÓÑEZ, D. y TOBÓN, C., 2020. Modelo JDL y calidad de la información para identificación biométrica a partir de señales multimodales: estudio exploratorio. *Revista Ibérica de Sistemas e Tecnologias de Informação*, no. E27, ISSN 16469895.

DAUGMAN, J., 2018. Iris Recognition. En: A.K. JAIN, P. FLYNN y A.A. ROSS (eds.), *Handbook of Biometrics* [en línea]. Boston, MA: Springer US, pp. 71-90. [consulta: 3 mayo 2023]. ISBN 978-0-387-71041-9. Disponible en: https://doi.org/10.1007/978-0-387-71041-9_4.

DÍAZ, J. y FLORES, G., 2019. *Diseño e implementación de prototipo de un sistema biométrico para mejorar el control de asistencia del personal docente en la FACFYM* [en línea]. Undergraduate Thesis. Lambayeque: Univiersidad Nacional Pedro Ruiz Gallo. [consulta: 28 abril 2023]. Disponible en: https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/4907/BC-TES-3742%20DIAZ%20COLLANTES%20-%20FLORES%20SORALUZ.pdf?sequence=1&isAllowed=y.

DUMITRESCU, C.-M., 2019. Combining Deep Learning Technologies with Multi-Level Gabor Features for Facial Recognition in Biometric Automated Systems. *Studies in Informatics and Control*, vol. 28, no. 2, ISSN 12201766. DOI 10.24846/v28i2y201910.

ELECTRONIC_IDENTIFICATION, 2021. Los estándares en la IDentificación

Electrónica: Verificación y sistemas. *Los estándares en la IDentificación Electrónica: Verificación y sistemas* [en línea]. [consulta: 3 mayo 2023]. Disponible en: https://www.electronicid.eu/es/blog/post/estandares-identificacion-electronica-verificacion/es.

GARRIDO IGLESIAS, R., BECKER CASTELLARO, S., GARRIDO IGLESIAS, R. y BECKER CASTELLARO, S., 2017. Biometrics in Chile and its risks. *Revista chilena de derecho y tecnología*, vol. 6, no. 1, ISSN 0719-2584. DOI 10.5354/0719-2584.2017.45825.

GASTELO, V. y CABRERA, J., 2019. *Propuesta para el diseño de un sistema de validación y autentificación biométrico dactilar para la asociación guadalupana* [en línea]. Undergraduate Thesis. Lima: Universidad Tecnológica del Perú. [consulta: 28 abril 2023]. Disponible en: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3890/Victor%20Gastelo_Junior%20Cabrera_Trabajo%20de%20Investigacion_Bachiller_2019.pdf?sequence=1&isAllowed=y.

GNIEWEK, P., SCHRECK, C.F. y HALLATSCHEK, O., 2019. Jamming by growth. En: arXiv:1810.01999 [cond-mat], *Physical Review Letters*, vol. 122, no. 20, ISSN 0031-9007, 1079-7114. DOI 10.1103/PhysRevLett.122.208102.

HERNÁNDEZ, R. y MENDOZA, C.P., 2018. *Metodología de la Investigación - Las rutas cualitativa, cuantitativa y mixta*. 9. México: McGRAW-HILL INTERAMERICANA EDITORES, S.A. ISBN 978-1-4562-6096-5.

HUESCA GONZÁLEZ, A.M.G.S., 2021. *Aspectos sociales en la seguridad ciudadana* [en línea]. S.l.: s.n. [consulta: 3 mayo 2023]. Disponible en: https://www.digitaliapublishing.com/a/100725/aspectos-sociales-en-la-seguridad-ciudadana.

IBM Documentation. [en línea], 2021. [consulta: 3 mayo 2023]. Disponible en: https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009740--htm.

JAIN, A.K. y ROSS, A., 2008. Introduction to Biometrics. En: A.K. JAIN, P.

FLYNN y A.A. ROSS (eds.), *Handbook of Biometrics* [en línea]. Boston, MA: Springer US, pp. 1-22. [consulta: 3 mayo 2023]. ISBN 978-0-387-71041-9. Disponible en: https://doi.org/10.1007/978-0-387-71041-9_1.

MALTONI, D. y CAPPELLI, R., 2018. Fingerprint Recognition. En: A.K. JAIN, P. FLYNN y A.A. ROSS (eds.), *Handbook of Biometrics* [en línea]. Boston, MA: Springer US, pp. 23-42. [consulta: 3 mayo 2023]. ISBN 978-0-387-71041-9. Disponible en: https://doi.org/10.1007/978-0-387-71041-9_2.

MINAEE, S., ABDOLRASHIDI, A., SU, H., BENNAMOUN, M. y ZHANG, D., 2019. *Biometrics recognition using deep learning: A survey* [en línea]. [consulta: 10 mayo 2023]. Disponible en: http://arxiv.org/abs/1912.00271.

MONTES, R.R., RICO, S., MOLANPHY, S., ADALMER, V. y MEJIA, V., 2018. ISACA glossary of terms English-Spanish. [en línea]. [consulta: 11 junio 2023]. Disponible en: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/isaca-glossary-english-spanish_mis_spa_0615.pdf.

PRESTON, A. y MA, K.-L., 2018. Cluster-Based Visualization for Merger Tree Data: The Challenge of Missing Expectations. *2018 IEEE Scientific Visualization Conference (SciVis)*. S.l.: s.n., pp. 42-46. DOI 10.1109/SciVis.2018.8823586.

RASOULI, H. y VALMOHAMMADI, C., 2020. Proposing a conceptual framework for customer identity and access management: A qualitative approach. *Global Knowledge, Memory and Communication*, vol. 69, no. 1/2, ISSN 25149342. DOI 10.1108/GKMC-02-2019-0014.

RATHGEB, C. y UHL, A., 2019. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, vol. 2011, no. 1, ISSN 1687-417X. DOI 10.1186/1687-417X-2011-3.

REYES PARRA, A. y VERÁSTEGUI GONZÁLES, F., 2018. Desarrollo prototipo de un sistema de informacion biometrico dactilar/Development prototype of a biometric information system dactilar. *Revista vinculos*, vol. 15, no. 2, ISSN 1794211X. DOI 10.14483/2322939X.13946.

ROSADO, S.G.P. y GUAÑA, E.P.R., 2018. Evaluación De La Eficiencia De Un Sistema De Control Biométrico Basado En La Norma Iso/Iec 9126-2 Y 9126-3. *3C TIC*, vol. 7, no. 4, DOI 10.17993/3ctic.0.00.60-75.

RUBENSTEIN, L., HEMPEL, S., MARGIE, D., ROSE, D., STOCKDALE, S., IDAMAY, C. y KIRSH, S., 2020. Eight Priorities for Improving Primary Care Access Management in Healthcare Organizations: Results of a Modified Delphi Stakeholder Panel. *Journal of General Internal Medicine*, vol. 35, no. 2, ISSN 08848734. DOI 10.1007/s11606-019-05541-2.

SÁNCHEZ CALLE, Á., 2005. *Aplicaciones de la visión artificial y la biometría informática*. Madrid: Dykinson. Actas, 5, ISBN 978-84-9982-272-3.

SAVVIDES, M., HEO, J. y PARK, S.W., 2018. Face Recognition. En: A.K. JAIN, P. FLYNN y A.A. ROSS (eds.), *Handbook of Biometrics* [en línea]. Boston, MA: Springer US, pp. 43-70. [consulta: 3 mayo 2023]. ISBN 978-0-387-71041-9. Disponible en: https://doi.org/10.1007/978-0-387-71041-9_3.

SERRATOSA, F., 2018. *La biometría para la identificación de las personas* [en línea]. S.l.: Universidad Oberta de Catalunya. [consulta: 3 mayo 2023]. Disponible en: https://openaccess.uoc.edu/bitstream/10609/70846/5/Biometr%C3%ADa_portada.pdf.

SIDLAUSKAS, D.P. y TAMER, S., 2018. Hand Geometry Recognition. *Handbook of Biometrics* [en línea]. S.l.: Springer, Boston, MA, pp. 91-107. [consulta: 4 mayo 2023]. Disponible en: https://link.springer.com/chapter/10.1007/978-0-387-71041-9_5.

TADLAOUI, S., 2018. *Manual de consultoría en asuntos públicos* [en línea]. S.l.: s.n. [consulta: 11 mayo 2023]. Disponible en: https://www.digitaliapublishing.com/a/39975/manual-de-consultoria-en-asuntos-publicos.

TROSHKOV, A.A., BOGDANOVA, S.V., ERMAKOVA, A.N. y RACHKOV, V.E., 2021. Designing a biometric access control concept. *IOP Conference*

Series. Materials Science and Engineering [en línea], vol. 1069, no. 1, [consulta: 28 abril 2023]. ISSN 17578981. DOI 10.1088/1757-899X/1069/1/012028. Disponible en: https://www.proquest.com/docview/2512931727/abstract/B9A2755D1F184A7EPQ/1.

WAYMAN, J., JAIN, A., MALTONI, D. y MAIO, D., 2019. *Biometric Systems: Technology, Design and Performance Evaluation*. London: Springer London. ISBN 978-1-85233-596-0.

ANEXOS

Anexo 1: Matriz de Operacionalización de variables

Título: Sistema de control biométrico para la gestión de accesos de empleados del Hospital MINSA – Moyobamba, 2023

Tabla 14. Matriz de operacionalización de la variable Sistema de control biométrico

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
Sistema de control biométrico	Los sistemas de control biométrico son sistemas automatizados que utilizan patrones para identificar o autenticar a una persona a través de sus características biométricas. (Wayman et al. 2019)	El sistema de control biométrico, será medido en función de las pruebas de funcionalidad de software, medidas en tiempo (minutos)	Prueba de caja negra	**Requerimientos funcionales:** ✓ Prueba funcional ✓ Prueba de estrés ✓ Prueba de rendimiento ✓ Prueba de usabilidad ✓ Prueba de seguridad ✓ Prueba de regresión ✓ Prueba de interoperabilidad	A razón.

Fuente: Elaboración propia

Tabla 15. Matriz de operacionalización de la variable Gestión de accesos

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
Gestión de accesos	La gestión de accesos se refiere al conjunto de procesos y herramientas que se utilizan para controlar y administrar el acceso a sistemas y recursos informáticos, como aplicaciones, bases de datos, archivos y redes, por parte de usuarios y grupos autorizados. (Villalón Millán, J.M)	La variable gestión de accesos se medirá mediante las dimensiones seguridad, privacidad, validación y eficiencia, medidas mediante escala de Lickert: Muy bajo, Bajo, Regular, Bueno, Muy bueno	Nivel de Seguridad	Nivel de seguridad en el procesamiento	Cualitativa ordinal
				Nivel de seguridad en el almacenamiento	
				Niveles de integridad	
				Niveles de confidencialidad	
			Nivel de Privacidad	Nivel de protección	
				Nivel de cifrado de datos	
				Nivel de retención y eliminación	
				Nivel de monitoreo	
			Nivel de Validación	Validación por nivel de acceso	
				Validación de precisión de datos	
				Validación de identidades falsas	
				Validación por fechas	

		Validación por turnos
	Nivel de Eficiencia	Monitoreo
		Retrasos innecesarios
		Rapidez del acceso
		Facilidad de uso

Fuente: Elaboración propia

Anexo 02: Instrumentos de recolección de datos

Instrumento 01. Prueba de caja negra: Sistema de control biométrico

Estimado/a participante:

Esta es una investigación llevada a cabo dentro de la escuela de Ingeniería de Sistemas, Programa de Formación para Adultos (PFA) de la Universidad César Vallejo; los datos recopilados son anónimos, serán tratados de forma confidencial respetando los principios de ética en la investigación y tienen finalidad estrictamente académica. Las fichas deben ser llenadas con la información obtenidas de la prueba de caja negra a nivel funcional, de equivalencia, de valor limite, de estrés, de rendimiento, de usabilidad, de seguridad, de regresión, de cumplimiento y de interoperabilidad.

PRUEBA FUNCIONAL

Tabla 16. Prueba funcional

Caso de Uso:	Prueba funcional		**N° 01**
Escenario:	Se realiza un conjunto de pruebas de reconocimiento de características biométricas		
Responsable:		Fecha:	
Precondiciones	N/A		
Datos de entrada:	Registro de datos biométricos de usuario		
Descripción de pasos:	1. Ingresar a la aplicación		
	2. Ingresar al módulo de registros biométricos de usuarios		
	3. Ingresar datos biométricos		
	4. Grabar datos		
	5. Realizar prueba reconocimiento biométrico		
Resultado esperado:	Se espera que, en menos de 3 segundos, el dispositivo biométrico se reconozca al usuario registrado		
Resultado obtenido:			
Recomendación:			
Errores:		Cumplimiento:	

PRUEBA DE ESTRÉS

Tabla 17. Prueba de estrés

Caso de Uso:	Prueba de estrés		**N° 02**
Escenario:	Se evalúa la capacidad del sistema para manejar una carga mayor que la carga típica, comprobar estabilidad bajo una alta demanda		
Responsable:		Fecha:	
Precondiciones	N/A		
Datos de entrada:	Ingresar un rango de fechas y seleccionar todas las áreas		
Descripción de pasos:	1. Ingresar a la aplicación		
	2. Ingresar al módulo de asistencia		
	3. Configurar el sistema para simular una alta carga de usuarios		
	4. Mantener una carga alta de usuarios en el sistema durante un período prolongado de tiempo		
	5. Comprobar si el sistema sigue funcionando de manera estable sin errores graves o caídas		
Resultado esperado:	El sistema responde frente a una carga incremental de entradas, limitado solo por el hardware.		
Resultado obtenido:			
Recomendación:			
Errores:		Cumplimiento:	

PRUEBA DE RENDIMIENTO

Tabla 18. Prueba de rendimiento

Caso de Uso:	Prueba rendimiento		**N° 03**
Escenario:	Se mide la velocidad y escalabilidad del sistema bajo una carga creciente		
Responsable:		Fecha:	
Precondiciones	N/A		
Datos de entrada:	Registro de usuarios y login		
Descripción de pasos:	1. Registrar el tiempo que lleva realizar tareas típicas, como el registro de usuarios y el inicio de sesión		
	2. Aumentar gradualmente la carga al registrar o iniciar sesión en más usuarios concurrentes		
	3. Someter el sistema a una carga máxima, simulando una alta demanda de usuarios concurrentes		
	4. Mantener una carga de usuarios durante un período prolongado para evaluar la estabilidad del sistema		
	5. Comprobar si se producen pérdidas de rendimiento o errores con el tiempo		
Resultado esperado:	El sistema responda de manera eficiente a las entradas.		
Resultado obtenido:			
Recomendación:			
Errores:		Cumplimiento:	

PRUEBA DE USABILIDAD

Tabla 19. Pruebas de usabilidad

Caso de Uso:	Prueba usabilidad		**N° 04**
Escenario:	Se evalúa la facilidad de uso y la eficiencia del proceso de registro en el sistema.		
Responsable:		Fecha:	
Precondiciones	N/A		
Datos de entrada:	Selección de usuarios de prueba		
Descripción de pasos:	1. Ingresar a la aplicación		
	2. Pedir a los usuarios que realicen las tareas y escenarios definidos mientras interactúan con el sistema		
	3. Registrar el tiempo que los llevó realizar cada tarea		
	4. Tomar nota sobre los inconvenientes que enfrentan los usuarios		
	5. Obtener opiniones sobre la experiencia del usuario		
Resultado esperado:	El sistema es entendible y fácil de usar.		
Resultado obtenido:			
Recomendación:			
Errores:		Cumplimiento:	

PRUEBA DE SEGURIDAD

Tabla 20. Prueba de seguridad

Caso de Uso:	Prueba seguridad		**N° 05**
Escenario:	Se realiza pruebas de seguridad del sistema		
Responsable:		Fecha:	
Precondiciones	N/A		
Datos de entrada:	Credenciales de acceso		
Descripción de pasos:	1. Asegurarse de que el sistema esté en un entorno de prueba seguro y replicable		
	2. Identificar las áreas del sistema que son críticas en términos de autenticación y acceso.		
	3. Evaluar la fortaleza de las contraseñas y asegurarse de que se almacenen de forma segura con técnicas de hash y salting		
	4. Utilizar herramientas de escaneo de vulnerabilidades		
	5. Realizar pruebas de inyección, como SQL Injection y Cross-Site Scripting (XSS)		
Resultado esperado:	El sistema demuestra ser confiable, integral y estar disponible, aun cuando es sometido a un ataque de fuerza bruta.		
Resultado obtenido:			
Recomendación:			
Errores:		Cumplimiento:	

PRUEBA DE REGRESIÓN

Tabla 21. Pruebas de regresión

Caso de Uso:	Prueba regresión		**N° 06**
Escenario:	Asegurar que las actualizaciones no causen fallos en funciones actuales		
Responsable:		Fecha:	
Precondiciones	N/A		
Datos de entrada:	Registro de datos personales		
Descripción de pasos:	1. Ingresar al módulo de personal		
	2. Se introduce nombre de personal, correo y DNI, etc. Válidos y se registrar correctamente		
	3. Se agrega una nueva función para la validación de un campo		
	4. Se vuelve a realizar la prueba de caja negra para este escenario de registro		
	5. Muestra mensaje de un error de no cumplir con la validación		
Resultado esperado:	Luego de una actualización. El sistema sigue funcionando de manera fluida y sin errores.		
Resultado obtenido:			
Recomendación:			
Errores:		Cumplimiento:	

PRUEBA DE INTEROPERABILIDAD

Tabla 22. Prueba de interoperabilidad

Caso de Uso:	Prueba de interoperabilidad		**N° 07**
Escenario:	Asegurar que el software web funcione correctamente en diferentes navegadores web		
Responsable:		Fecha:	
Precondiciones	N/A		
Datos de entrada:	Credenciales de acceso		
Descripción de pasos:	1. Identificar una lista de navegadores web populares que deseas probar.		
	2. Iniciar sesión en el software web en cada navegador seleccionado.		
	3. Realizar tareas comunes, como navegar por la interfaz, ingresar registros.		
	4. Verificar que todas las funcionalidades del software web.		
	5. El software web es compatible con dispositivos móviles		
Resultado esperado:	El sistema funciona independientemente del sistema operativo		
Resultado obtenido:			
Recomendación:			
Errores:		Cumplimiento:	

Instrumento 02. Cuestionario: Gestión de accesos

Estimado/a participante:

Esta es una investigación llevada a cabo dentro de la escuela de Ingeniería de Sistemas, Programa de Formación para Adultos (PFA) de la Universidad César Vallejo; los datos recopilados son anónimos, serán tratados de forma confidencial respetando los principios de ética en la investigación y tienen finalidad estrictamente académica. Por tanto, se le pide que de forma voluntaria contribuya a llenar el siguiente cuestionario, para lo cual debe marcar una de las siguientes alternativas donde a cada número le corresponde los siguientes valores:

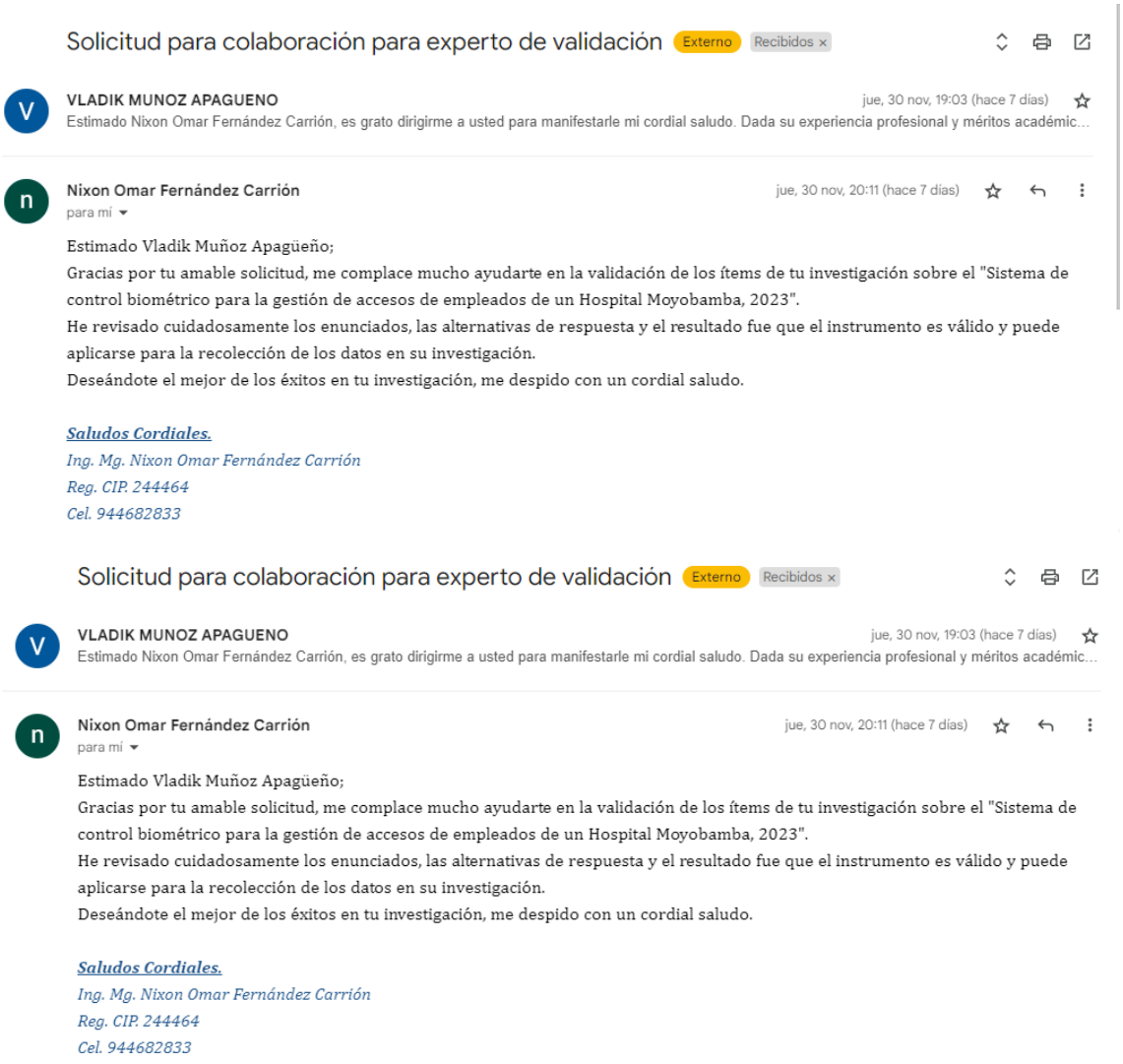
1: Muy bajo
2: Bajo
3: Regular
4: Bueno
5: Muy bueno

N°	Ítems	1	2	3	4	5
Nivel de seguridad						
01	¿Cómo califica el nivel de seguridad en el procesamiento de los datos de los usuarios?					
02	¿Cómo califica el nivel de seguridad en el almacenamiento de los datos de los usuarios?					
03	¿Cómo califica el nivel de integridad de los datos almacenados en el sistema de gestión de accesos?					
04	¿Cómo califica el nivel de confidencialidad de los datos almacenados en el sistema de gestión de accesos?					
Nivel de privacidad						
05	¿Cómo califica el nivel de protección de sus datos personales?					
06	¿Cómo califica el nivel de cifrado de datos utilizado en la gestión de accesos para proteger la información del personal?					
07	¿Cómo califica la privacidad en la retención y eliminación de los datos biométricos cuando ya no son necesarios?					
08	¿Cómo califica el nivel de monitoreo para detectar posibles violaciones de privacidad en el manejo de los datos utilizados en la gestión de accesos?					

Nivel de validación						
09	¿Cómo califica el nivel de validación de la identidad de los usuarios antes de otorgarles acceso a los sistemas o recursos de la institución?					
10	¿Cómo califica el nivel de precisión en la corrección de errores en la identificación de los trabajadores?					
11	¿Cómo califica el nivel de manejo de identidades falsas o intentos de suplantación de identidad en el proceso de gestión de accesos?					
12	¿Cómo califica el nivel de validación de accesos a la institución por fechas?					
13	¿Cómo califica el nivel de validación de accesos a la institución por turnos?					
Nivel de eficiencia						
14	¿Cómo califica el nivel de eficiencia en el monitoreo de casos atípicos en el acceso del personal?					
15	¿Cómo califica la cantidad de retrasos innecesarios en el registro del personal para acceder o salir de la institución?					
16	¿Cómo califica la rapidez de acceso a la institución?					
17	¿Cómo califica el nivel de usabilidad del mecanismo utilizado en la actualidad para registro de personal?					

Anexo 03: Solicitud de validación de contenido de la guía de Observación y cuestionario

Anexo: Solicitud como juez experto



Solicitud para colaboración para experto de validación Externo Recibidos ×

VLADIK MUNOZ APAGUENO jue, 30 nov, 19:03 (hace 7 días)
Estimado Nixon Omar Fernández Carrión, es grato dirigirme a usted para manifestarle mi cordial saludo. Dada su experiencia profesional y méritos académic...

Nixon Omar Fernández Carrión jue, 30 nov, 20:11 (hace 7 días)
para mí

Estimado Vladik Muñoz Apagüeño;
Gracias por tu amable solicitud, me complace mucho ayudarte en la validación de los ítems de tu investigación sobre el "Sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023".
He revisado cuidadosamente los enunciados, las alternativas de respuesta y el resultado fue que el instrumento es válido y puede aplicarse para la recolección de los datos en su investigación.
Deseándote el mejor de los éxitos en tu investigación, me despido con un cordial saludo.

Saludos Cordiales.
Ing. Mg. Nixon Omar Fernández Carrión
Reg. CIP. 244464
Cel. 944682833

Solicitud para colaboración para experto de validación Externo Recibidos ×

VLADIK MUNOZ APAGUENO jue, 30 nov, 19:03 (hace 7 días)
Estimado Nixon Omar Fernández Carrión, es grato dirigirme a usted para manifestarle mi cordial saludo. Dada su experiencia profesional y méritos académic...

Nixon Omar Fernández Carrión jue, 30 nov, 20:11 (hace 7 días)
para mí

Estimado Vladik Muñoz Apagüeño;
Gracias por tu amable solicitud, me complace mucho ayudarte en la validación de los ítems de tu investigación sobre el "Sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023".
He revisado cuidadosamente los enunciados, las alternativas de respuesta y el resultado fue que el instrumento es válido y puede aplicarse para la recolección de los datos en su investigación.
Deseándote el mejor de los éxitos en tu investigación, me despido con un cordial saludo.

Saludos Cordiales.
Ing. Mg. Nixon Omar Fernández Carrión
Reg. CIP. 244464
Cel. 944682833

Solicito Validación como Juez experto

Externo Recibidos ×

WILSON DIAZ BUSTAMANTE <ddiazbu@ucvvirtual.edu.pe> mar, 3 oct, 9:08 (hace 4 días)

para jramirezmelendez

Estimado Mg. Ing. Sist. Jaime Paolo Ramírez Melendez, es grato dirigirme a usted para manifestarle mi cordial saludo.
Dada su experiencia profesional y méritos académicos y personales, le solicitó su imprescindible colaboración como experto para la validación de conteni los ítems que conforman los instrumentos de recolección de datos; que serán aplicados a la muestra seleccionada que tiene como finalidad recoger información directa para la investigación titulada: "Sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2(Para efectuar la validación del instrumento, usted deberá leer cuidadosamente cada enunciado y sus correspondientes alternativas de respuesta, es donc pueden seleccionar, una, varias o ninguna alternativa de acuerdo al criterio personal y profesional que corresponda al instrumento.

Se le agradece cualquier sugerencia relativa a la redacción, el contenido, la pertinencia y congruencia u otro aspecto que considere relevante para mejora mismo.

Atte.

Jaime Paolo Ramirez Melendez 3 oct 2023, 11:27 (hace 4 días)

para mi

Buen Dia Sr Wilson Diaz Bustamante

La presente es para confirmar que he revisado sus instrumentos de validación. Llegando a la conclusión que el Instrumento es Válido y puede aplicarse para la recolección de datos de su investigación.

Sin otro particular.

Atentamente

Mg. Jaime Paolo Ramirez Melendez

•••

--

ING. JAIME PAOLO RAMIREZ MELENDEZ
MOVIL. 942609888

Solicitud para validación colaboración para experto de validación

Externo Recibidos ×

VLADIK MUNOZ APAGUENO <mmunozap@ucvvirtual.edu.pe> mar, 20 jun, 13:30

para roman10_1

Estimado Miguel Ángel, es grato dirigirme a usted para manifestarle mi cordial saludo.
Dada su experiencia profesional y méritos académicos y personales, le solicito su imprescindible colaboración como experto para la validación de contenido de los ítems que conforman los instrumentos de recolección de datos; que serán aplicados a la muestra seleccionada que tiene como finalidad recoger información directa para la investigación titulada: "Sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023".
Para efectuar la validación del instrumento, usted deberá leer cuidadosamente cada enunciado y sus correspondientes alternativas de respuesta, es donde se pueden seleccionar, una, varias o ninguna alternativa de acuerdo al criterio personal y profesional que corresponda al instrumento.

Se le agradece cualquier sugerencia relativa a la redacción, el contenido, la pertinencia y congruencia u otro aspecto que considere relevante para mejorar el mismo.

Atentamente:
Vladik Muñoz Apagüeño

Miguel martinez garcía mar, 3 oct, 20:00 (hace 11 días)

para mi

Estimado Vladik Muñoz Apagueño;
Gracias por tu amable solicitud, me complace mucho ayudarte en la validación de los ítems de tu investigación sobre el "Sistema de control biométrico para la gestión de accesos de empleados de un Hospital Moyobamba, 2023".
He revisado cuidadosamente los enunciados, las alternativas de respuesta y el resultado fue que el instrumento es válido y puede aplicarse para la recolección de los datos en su investigación.

Deseándote el mejor de los éxitos en tu investigación, me despido con un cordial saludo.

Att:

Ing. Mstr. Miguel Angel Roman Martínez García

Anexo 04: Validación de contenido de la guía de Observación y cuestionario: Base de datos de Prueba piloto para la Confiabilidad.

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento Ficha de observación: **Pruebas Funcionales** y Cuestionario: **Gestión de accesos,** La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando a los sistemas de información. Agradecemos su valiosa colaboración.

1. **Datos generales del juez**

Nombre del juez:	Nixon Omar Fernández Carrión
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional (X)
Áreas de experiencia profesional:	Docente en la Escuela Profesional de Ingeniería
Institución donde labora:	Universidad Católica Sedes Sapientiae – Filial Rioja
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)

2. **Propósito de la evaluación:**
Validar el contenido del instrumento, por juicio de expertos.

3. **Datos de la escala**

Nombre de la prueba:	Validación de experto
Autores:	Wilson Díaz Bustamante, Vladik Muñoz Apagüeño
Procedencia:	Universidad Cesar Vallejo -Tarapoto
Administración:	Presencial
Tiempo de aplicación:	10 - 15 minutos
Ámbito de aplicación:	En un Hospital de la provincia de Moyobamba
Significación:	Explicar cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

4. **Soporte teórico**

FICHA DE OBSERVACION – Variable Sistema de control biométrico
Los sistemas de control biométrico son sistemas automatizados que utilizan patrones para identificar o autenticar a una persona a través de sus características biométricas.
(Wayman et al. 2019)
El sistema de control biométrico será medido en función de las pruebas de funcionalidad de

software, medidas en tiempo.

Escala	Dimensiones	Indicadores
A razón.	Prueba de caja negra	Prueba funcional
		Prueba de estrés
		Prueba de rendimiento
		Prueba de usabilidad
		Prueba de seguridad
		Prueba de regresión
		Prueba de interoperabilidad

CUESTIONARIO – Variable gestión de accesos

La gestión de accesos se refiere al conjunto de procesos y herramientas que se utilizan para controlar y administrar el acceso a sistemas y recursos informáticos, como aplicaciones, bases de datos, archivos y redes, por parte de usuarios y grupos autorizados.
(Villalón Millán, J.M)

La variable gestión de accesos se medirá mediante las dimensiones seguridad, privacidad, validación y eficiencia

Escala	Dimensiones	Indicadores
Cualitativa ordinal	Nivel de Seguridad	Nivel de seguridad en el procesamiento
		Nivel de seguridad en el almacenamiento
		Niveles de integridad
		Niveles de confidencialidad
	Nivel de Privacidad	Nivel de protección
		Nivel de cifrado de datos
		Nivel de retención y eliminación
		Nivel de monitoreo
	Nivel de Validación	Validación por nivel de acceso
		Validación de precisión de datos
		Validación de identidades falsas
		Validación por fechas
		Validación por turnos
	Nivel de Eficiencia	Monitoreo
		Retrasos innecesarios
		Rapidez del acceso
		Facilidad de uso

5. <u>Presentación de instrucciones para el juez</u>:

A continuación a usted le presento el cuestionario: "Gestión de accesos" elaborado por Wilson Díaz Bustamante, Vladik Muñoz Apagüeño en el año 2023 De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

VARIABLE: SISTEMA DE CONTROL BIOMÉTRICO

Dimensión: Pruebas de caja negra

Objetivo: Evaluar exhaustivamente la robustez, confiabilidad y adecuación del sistema mediante pruebas de caja negra, con el propósito de identificar y mitigar posibles fallos, optimizar el rendimiento, garantizar la seguridad, validar la funcionalidad, la usabilidad, la interoperabilidad y la capacidad de recuperación del sistema bajo diferentes condiciones, con el fin de mejorar la calidad general y la experiencia del usuario.

Casos de Uso / Pruebas		Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Caso de Uso: N° 01	**PRUEBA FUNCIONAL**	5	5	4	
Descripción de pasos:	1. Ingresar a la aplicación				
	2. Ingresar al módulo de registros biométricos de usuarios				
	3. Ingresar datos biométricos				
	4. Grabar datos				
	5. Realizar prueba reconocimiento biométrico				
Resultado esperado:	Se espera que, en menos de 3 segundos, el dispositivo biométrico se reconozca al usuario registrado.				
Resultado obtenido:					
Caso de Uso: N° 02	**PRUEBA DE ESTRÉS**	5	4	5	
Descripción de pasos:	1. Ingresar a la aplicación				
	2. Ingresar al módulo de asistencia				
	3. Configurar el sistema para simular una alta carga de usuarios				
	4. Mantener una carga alta de usuarios en el sistema durante un período prolongado de tiempo				
	5. Comprobar si el sistema sigue funcionando de manera estable sin errores graves o caídas				
Resultado esperado:	El sistema responde frente a una carga incremental de entradas, limitado solo por el hardware.				
Resultado obtenido:					
Caso de Uso: N° 03	**PRUEBA DE RENDIMIENTO**	5	5	5	
Descripción de pasos:	Registro de usuarios y login				
	1. Registrar el tiempo que lleva realizar tareas típicas, como el registro de usuarios y el inicio de sesión				

	2. Aumentar gradualmente la carga al registrar o iniciar sesión en más usuarios concurrentes				
	3. Someter el sistema a una carga máxima, simulando una alta demanda de usuarios concurrentes				
	4. Mantener una carga de usuarios durante un período prolongado para evaluar la estabilidad del sistema				
Resultado esperado:	El sistema responda de manera eficiente a las entradas.				
Resultado obtenido:					
Caso de Uso: N° 04	**PRUEBA DE USABILIDAD**	4	5	5	
Descripción de pasos:	Selección de usuarios de prueba				
	1. Ingresar a la aplicación				
	2. Pedir a los usuarios que realicen las tareas y escenarios definidos mientras interactúan con el sistema				
	3. Registrar el tiempo que los llevó realizar cada tarea				
	4. Tomar nota sobre los inconvenientes que enfrentan los usuarios				
Resultado esperado:	El sistema es entendible y fácil de usar.				
Resultado obtenido:					
Caso de Uso: N° 05	**PRUEBA DE SEGURIDAD**	5	5	5	
Descripción de pasos:	1. Asegurarse de que el sistema esté en un entorno de prueba seguro y replicable				
	2. Identificar las áreas del sistema que son críticas en términos de autenticación y acceso.				
	3. Evaluar la fortaleza de las contraseñas y asegurarse de que se almacenen de forma segura con técnicas de hash y salting				
	4. Utilizar herramientas de escaneo de vulnerabilidades				
	5. Realizar pruebas de inyección, como SQL Injection y Cross-Site Scripting (XSS)				

Resultado esperado:	El sistema demuestra ser confiable, integral y estar disponible, aun cuando es sometido a un ataque de fuerza bruta.				
Resultado obtenido:					
Caso de Uso: N° 06	**PRUEBA DE REGRESIÓN**	5	5	5	
Descripción de pasos:	1. Ingresar al módulo de personal				
	2. Se introduce nombre de personal, correo y DNI, etc. Válidos y se registrar correctamente				
	3. Se agrega una nueva función para la validación de un campo				
	4. Se vuelve a realizar la prueba de caja negra para este escenario de registro				
	5. Muestra mensaje de un error de no cumplir con la validación				
Resultado esperado:	Luego de una actualización. El sistema sigue funcionando de manera fluida y sin errores.				
Resultado obtenido:					
Caso de Uso: N° 07	**PRUEBA DE INTEROPERABILIDAD**	5	4	5	
Descripción de pasos:	1. Identificar una lista de navegadores web populares que deseas probar.				
	2. Iniciar sesión en el software web en cada navegador seleccionado.				
	3. Realizar tareas comunes, como navegar por la interfaz, ingresar registros.				
	4. Verificar que todas las funcionalidades del software web.				
	5. El software web es compatible con dispositivos móviles				
Resultado esperado:	El sistema funciona independientemente del sistema operativo				
Resultado obtenido:					

VARIABLE: GESTIÓN DE ACCESOS

Dimensión: Nivel de Seguridad

Objetivo: Evaluar y medir el nivel de protección y resistencia ante intentos de acceso no autorizados al sistema biométrico, considerando medidas de cifrado, autenticación y detección de intrusos para garantizar la integridad y confidencialidad de los datos biométricos.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Nivel de seguridad en el procesamiento	5	5	5	
Nivel de seguridad en el almacenamiento	5	5	4	
Niveles de integridad	5	4	5	
Niveles de confidencialidad	5	5	5	

Dimensión: Nivel de Privacidad

Objetivo: Analizar y cuantificar la salvaguarda de la información personal y biométrica de los individuos registrados en el sistema, evaluando las políticas de privacidad implementadas, el control de acceso a datos sensibles y las medidas para prevenir su mal uso o divulgación no autorizada.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Nivel de protección	5	5	5	
Nivel de cifrado de datos	5	5	5	
Nivel de retención y eliminación	5	5	4	
Nivel de monitoreo	5	5	5	

Dimensión: Nivel de Validación.

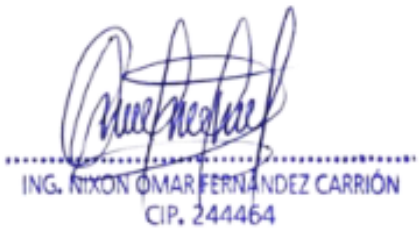
Objetivo: Determinar y verificar la precisión y fiabilidad del sistema biométrico mediante pruebas exhaustivas que validen la identificación correcta de los usuarios autorizados y la minimización de errores de identificación, considerando tasas de falsa aceptación y falsa rechazo.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Validación por nivel de acceso	5	5	5	
Validación de precisión de datos	5	5	5	
Validación de identidades falsas	4	5	5	
Validación por fechas	5	4	5	
Validación por turnos	5	5	5	

Dimensión: Nivel de Eficiencia

Objetivo: Medir la efectividad y eficiencia operativa del sistema biométrico en términos de velocidad de identificación, capacidad de procesamiento y rendimiento en tiempo real, considerando la optimización de recursos y la respuesta rápida ante las demandas del sistema.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Monitoreo	5	5	5	
Retrasos innecesarios	5	5	4	
Rapidez del acceso	5	5	5	
Facilidad de uso	5	5	5	



ING. NIXON OMAR FERNÁNDEZ CARRIÓN
CIP. 244464

Nombre del juez:	RAMIREZ MELENDEZ JAIME PAOLO
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (X)
Áreas de experiencia profesional:	GESTION PUBLICA, SISTEMAS DE SALUD
Institución donde labora:	DIRECCION REGIONAL DE SALUD
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)

VARIABLE: SISTEMA DE CONTROL BIOMÉTRICO

Dimensión: Pruebas de caja negra

Objetivo: Evaluar exhaustivamente la robustez, confiabilidad y adecuación del sistema mediante pruebas de caja negra, con el propósito de identificar y mitigar posibles fallos, optimizar el rendimiento, garantizar la seguridad, validar la funcionalidad, la usabilidad, la interoperabilidad y la capacidad de recuperación del sistema bajo diferentes condiciones, con el fin de mejorar la calidad general y la experiencia del usuario.

Casos de Uso / Pruebas		**Claridad**	**Coherencia**	**Relevancia**	**Observaciones/ Recomendaciones**
Caso de Uso: N° 01	**PRUEBA FUNCIONAL**	5	5	5	
Descripción de pasos:	1. Ingresar a la aplicación				
	2. Ingresar al módulo de registros biométricos de usuarios				
	3. Ingresar datos biométricos				
	4. Grabar datos				
	5. Realizar prueba reconocimiento biométrico				
Resultado esperado:	Se espera que, en menos de 3 segundos, el dispositivo biométrico se reconozca al usuario registrado.				
Resultado obtenido:					
Caso de Uso: N° 02	**PRUEBA DE ESTRÉS**	5	5	5	
Descripción de pasos:	1. Ingresar a la aplicación				
	2. Ingresar al módulo de asistencia				
	3. Configurar el sistema para simular una alta carga de usuarios				

	4. Mantener una carga alta de usuarios en el sistema durante un período prolongado de tiempo				
	5. Comprobar si el sistema sigue funcionando de manera estable sin errores graves o caídas				
Resultado esperado:	El sistema responde frente a una carga incremental de entradas, limitado solo por el hardware.				
Resultado obtenido:					
Caso de Uso: N° 03	**PRUEBA DE RENDIMIENTO**	5	5	5	
Descripción de pasos:	Registro de usuarios y login				
	1. Registrar el tiempo que lleva realizar tareas típicas, como el registro de usuarios y el inicio de sesión				
	2. Aumentar gradualmente la carga al registrar o iniciar sesión en más usuarios concurrentes				
	3. Someter el sistema a una carga máxima, simulando una alta demanda de usuarios concurrentes				
	4. Mantener una carga de usuarios durante un período prolongado para evaluar la estabilidad del sistema				
Resultado esperado:	El sistema responda de manera eficiente a las entradas.				
Resultado obtenido:					
Caso de Uso: N° 04	**PRUEBA DE USABILIDAD**	5	5	5	
Descripción de pasos:	Selección de usuarios de prueba				
	1. Ingresar a la aplicación				
	2. Pedir a los usuarios que realicen las tareas y escenarios definidos mientras interactúan con el sistema				
	3. Registrar el tiempo que los llevó realizar cada tarea				
	4. Tomar nota sobre los inconvenientes que enfrentan los usuarios				
Resultado esperado:	El sistema es entendible y fácil de usar.				
Resultado obtenido:					
Caso de Uso: N° 05	**PRUEBA DE SEGURIDAD**	5	5	5	

Descripción de pasos:	1. Asegurarse de que el sistema esté en un entorno de prueba seguro y replicable				
	2. Identificar las áreas del sistema que son críticas en términos de autenticación y acceso.				
	3. Evaluar la fortaleza de las contraseñas y asegurarse de que se almacenen de forma segura con técnicas de hash y salting				
	4. Utilizar herramientas de escaneo de vulnerabilidades				
	5. Realizar pruebas de inyección, como SQL Injection y Cross-Site Scripting (XSS)				
Resultado esperado:	El sistema demuestra ser confiable, integral y estar disponible, aun cuando es sometido a un ataque de fuerza bruta.				
Resultado obtenido:					
Caso de Uso: N° 06	**PRUEBA DE REGRESIÓN**	5	5	5	
Descripción de pasos:	1. Ingresar al módulo de personal				
	2. Se introduce nombre de personal, correo y DNI, etc. Válidos y se registrar correctamente				
	3. Se agrega una nueva función para la validación de un campo				
	4. Se vuelve a realizar la prueba de caja negra para este escenario de registro				
	5. Muestra mensaje de un error de no cumplir con la validación				
Resultado esperado:	Luego de una actualización. El sistema sigue funcionando de manera fluida y sin errores.				
Resultado obtenido:					
Caso de Uso: N° 07	**PRUEBA DE INTEROPERABILIDAD**	5	5	5	
Descripción de pasos:	1. Identificar una lista de navegadores web populares que deseas probar.				
	2. Iniciar sesión en el software web en cada navegador seleccionado.				
	3. Realizar tareas comunes, como navegar por la interfaz, ingresar registros.				

	4. Verificar que todas las funcionalidades del software web.				
	5. El software web es compatible con dispositivos móviles				
Resultado esperado:	El sistema funciona independientemente del sistema operativo				
Resultado obtenido:					

VARIABLE: GESTIÓN DE ACCESOS

Dimensión: Nivel de Seguridad

Objetivo: Evaluar y medir el nivel de protección y resistencia ante intentos de acceso no autorizados al sistema biométrico, considerando medidas de cifrado, autenticación y detección de intrusos para garantizar la integridad y confidencialidad de los datos biométricos.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Nivel de seguridad en el procesamiento	5	5	5	
Nivel de seguridad en el almacenamiento	5	5	5	
Niveles de integridad	5	5	5	
Niveles de confidencialidad	5	5	5	

Dimensión: Nivel de Privacidad

Objetivo: Analizar y cuantificar la salvaguarda de la información personal y biométrica de los individuos registrados en el sistema, evaluando las políticas de privacidad implementadas, el control de acceso a datos sensibles y las medidas para prevenir su mal uso o divulgación no autorizada.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones

Nivel de protección	5	5	5	
Nivel de cifrado de datos	5	5	5	
Nivel de retención y eliminación	4	4	4	
Nivel de monitoreo	5	5	5	

Dimensión: Nivel de Validación.

Objetivo: Determinar y verificar la precisión y fiabilidad del sistema biométrico mediante pruebas exhaustivas que validen la identificación correcta de los usuarios autorizados y la minimización de errores de identificación, considerando tasas de falsa aceptación y falsa rechazo.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Validación por nivel de acceso	5	5	5	
Validación de precisión de datos	5	5	5	
Validación de identidades falsas	5	5	5	
Validación por fechas	5	5	5	
Validación por turnos	5	5	5	

Dimensión: Nivel de Eficiencia

Objetivo: Medir la efectividad y eficiencia operativa del sistema biométrico en términos de velocidad de identificación, capacidad de procesamiento y rendimiento en tiempo real, considerando la optimización de recursos y la respuesta rápida ante las demandas del sistema.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Monitoreo	5	5	5	
Retrasos innecesarios	5	4	4	
Rapidez del acceso	5	5	5	
Facilidad de uso	5	5	5	

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento Ficha de observación: **Pruebas Funcionales** y Cuestionario: **Gestión de accesos,** La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando a los sistemas de información. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Miguel Ángel Ramón Martínez García
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (X)
Áreas de experiencia profesional:	Tecnología de la Información
Institución donde labora:	Poder Judicial
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala

Nombre de la prueba:	Validación de experto
Autores:	Wilson Díaz Bustamante, Vladik Muñoz Apagüeño
Procedencia:	Universidad Cesar Vallejo -Tarapoto
Administración:	Presencial
Tiempo de aplicación:	10 - 15 minutos
Ámbito de aplicación:	En un Hospital de la provincia de Moyobamba
Significación:	Explicar cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

4. Soporte teórico

FICHA DE OBSERVACION – Variable Sistema de control biométrico

Los sistemas de control biométrico son sistemas automatizados que utilizan patrones para identificar o autenticar a una persona a través de sus características biométricas. (Wayman et al. 2019).

El sistema de control biométrico será medido en función de las pruebas de funcionalidad de software, medidas en tiempo.

VARIABLE: SISTEMA DE CONTROL BIOMÉTRICO

Dimensión: Pruebas de caja negra

Objetivo: Evaluar exhaustivamente la robustez, confiabilidad y adecuación del sistema mediante pruebas de caja negra, con el propósito de identificar y mitigar posibles fallos, optimizar el rendimiento, garantizar la seguridad, validar la funcionalidad, la usabilidad, la interoperabilidad y la capacidad de recuperación del sistema bajo diferentes condiciones, con el fin de mejorar la calidad general y la experiencia del usuario.

Casos de Uso / Pruebas		Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Caso de Uso: N° 01	**PRUEBA FUNCIONAL**	5	5	5	
Descripción de pasos:	1. Ingresar a la aplicación				
	2. Ingresar al módulo de registros biométricos de usuarios				
	3. Ingresar datos biométricos				
	4. Grabar datos				
	5. Realizar prueba reconocimiento biométrico				
Resultado esperado:	Se espera que, en menos de 3 segundos, el dispositivo biométrico se reconozca al usuario registrado.				
Resultado obtenido:					
Caso de Uso: N° 02	**PRUEBA DE ESTRÉS**	5	5	5	
Descripción de pasos:	1. Ingresar a la aplicación				
	2. Ingresar al módulo de asistencia				
	3. Configurar el sistema para simular una alta carga de usuarios				
	4. Mantener una carga alta de usuarios en el sistema durante un período prolongado de tiempo				
	5. Comprobar si el sistema sigue funcionando de manera estable sin errores graves o caídas				
Resultado esperado:	El sistema responde frente a una carga incremental de entradas, limitado solo por el hardware.				
Resultado obtenido:					
Caso de Uso: N° 03	**PRUEBA DE RENDIMIENTO**	5	5	5	
Descripción de pasos:	Registro de usuarios y login				
	1. Registrar el tiempo que lleva realizar tareas típicas, como el registro de usuarios y el inicio de sesión				

	2. Aumentar gradualmente la carga al registrar o iniciar sesión en más usuarios concurrentes				
	3. Someter el sistema a una carga máxima, simulando una alta demanda de usuarios concurrentes				
	4. Mantener una carga de usuarios durante un período prolongado para evaluar la estabilidad del sistema				
Resultado esperado:	El sistema responda de manera eficiente a las entradas.				
Resultado obtenido:					
Caso de Uso: N° 04	**PRUEBA DE USABILIDAD**				
Descripción de pasos:	Selección de usuarios de prueba	5	5	5	
	1. Ingresar a la aplicación				
	2. Pedir a los usuarios que realicen las tareas y escenarios definidos mientras interactúan con el sistema				
	3. Registrar el tiempo que los llevó realizar cada tarea				
	4. Tomar nota sobre los inconvenientes que enfrentan los usuarios				
Resultado esperado:	El sistema es entendible y fácil de usar.				
Resultado obtenido:					
Caso de Uso: N° 05	**PRUEBA DE SEGURIDAD**				
Descripción de pasos:	1. Asegurarse de que el sistema esté en un entorno de prueba seguro y replicable	5	5	5	
	2. Identificar las áreas del sistema que son críticas en términos de autenticación y acceso.				
	3. Evaluar la fortaleza de las contraseñas y asegurarse de que se almacenen de forma segura con técnicas de hash y salting				
	4. Utilizar herramientas de escaneo de vulnerabilidades				
	5. Realizar pruebas de inyección, como SQL Injection y Cross-Site Scripting (XSS)				

Resultado esperado:	El sistema demuestra ser confiable, integral y estar disponible, aun cuando es sometido a un ataque de fuerza bruta.				
Resultado obtenido:					
Caso de Uso: N° 06	**PRUEBA DE REGRESIÓN**				
Descripción de pasos:	1. Ingresar al módulo de personal 2. Se introduce nombre de personal, correo y DNI, etc. Válidos y se registrar correctamente 3. Se agrega una nueva función para la validación de un campo 4. Se vuelve a realizar la prueba de caja negra para este escenario de registro 5. Muestra mensaje de un error de no cumplir con la validación	5	5	5	
Resultado esperado:	Luego de una actualización. El sistema sigue funcionando de manera fluida y sin errores.				
Resultado obtenido:					
Caso de Uso: N° 07	**PRUEBA DE INTEROPERABILIDAD**				
Descripción de pasos:	1. Identificar una lista de navegadores web populares que deseas probar. 2. Iniciar sesión en el software web en cada navegador seleccionado. 3. Realizar tareas comunes, como navegar por la interfaz, ingresar registros. 4. Verificar que todas las funcionalidades del software web. 5. El software web es compatible con dispositivos móviles	5	5	5	
Resultado esperado:	El sistema funciona independientemente del sistema operativo				
Resultado obtenido:					

Mg. Miguel Angel Acosta Martinez Garro
ING. DE SISTEMAS
CIP. CDSM N° 222504

VARIABLE: GESTIÓN DE ACCESOS

Dimensión: Nivel de Seguridad

Objetivo: Evaluar y medir el nivel de protección y resistencia ante intentos de acceso no autorizados al sistema biométrico, considerando medidas de cifrado, autenticación y detección de intrusos para garantizar la integridad y confidencialidad de los datos biométricos.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Nivel de seguridad en el procesamiento	5	5	5	
Nivel de seguridad en el almacenamiento	5	5	5	
Niveles de integridad	5	5	5	
Niveles de confidencialidad	5	5	5	

Dimensión: Nivel de Privacidad

Objetivo: Analizar y cuantificar la salvaguarda de la información personal y biométrica de los individuos registrados en el sistema, evaluando las políticas de privacidad implementadas, el control de acceso a datos sensibles y las medidas para prevenir su mal uso o divulgación no autorizada.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Nivel de protección	4	4	5	
Nivel de cifrado de datos	5	5	5	
Nivel de retención y eliminación	5	5	5	
Nivel de monitoreo	4	5	5	

Dimensión: Nivel de Validación.

Objetivo: Determinar y verificar la precisión y fiabilidad del sistema biométrico mediante pruebas exhaustivas que validen la identificación correcta de los usuarios autorizados y la minimización de errores de identificación, considerando tasas de falsa aceptación y falsa rechazo.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Validación por nivel de acceso	5	5	5	
Validación de precisión de datos	4	5	5	
Validación de identidades falsas	4	4	5	
Validación por fechas	5	5	5	
Validación por turnos	5	5	5	

Dimensión: Nivel de Eficiencia

Objetivo: Medir la efectividad y eficiencia operativa del sistema biométrico en términos de velocidad de identificación, capacidad de procesamiento y rendimiento en tiempo real, considerando la optimización de recursos y la respuesta rápida ante las demandas del sistema.

INDICADORES	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Monitoreo	4	4	5	
Retrasos innecesarios	5	5	5	
Rapidez del acceso	5	5	5	
Facilidad de uso	5	5	5	

Mg. Miguel Angel Acosta Martinez Garcia
ING. DE SISTEMAS
CIP. COSM N° 222504

Alfa de Cronbach

		N	%
Casos	Válido	10	100,0
	Excluido[a]	0	,0
	Total	10	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,759	17

Empl.	*Item 1*	*Item 2*	*Item 3*	*Item 4*	*Item 5*	*Item 6*	*Item 7*	*Item 8*	*Item 9*	*Item 10*	*Item 11*	*Item 12*	*Item 13*	*Item 14*	*Item 15*	*Item 16*	*Item 17*	*Total*
1	3	3	4	4	3	3	4	4	5	2	3	2	4	3	4	3	4	58
2	4	5	5	2	3	4	4	5	3	3	5	4	5	4	4	4	4	68
3	3	2	4	3	4	2	4	3	2	5	4	2	2	3	3	3	2	51
4	4	3	4	5	4	3	2	5	4	5	3	3	4	3	4	5	4	65
5	3	3	3	3	2	3	2	4	2	4	5	4	3	4	4	4	2	55
6	4	3	4	2	4	2	3	4	1	3	4	2	2	2	2	3	3	48
7	3	4	2	4	3	3	4	3	4	4	2	1	3	2	3	4	5	54
8	3	4	2	3	4	4	4	5	5	4	5	5	4	5	4	3	3	67
9	5	4	4	4	4	2	4	4	5	5	4	4	4	4	3	5	4	69
10	5	3	5	4	4	4	3	3	3	2	3	3	4	3	3	4	5	61
Varianzas	0.61	0.64	1.01	0.84	0.45	0.60	0.64	0.60	1.84	1.21	0.96	1.40	0.85	0.81	0.44	0.56	1.04	50.84

Anexo 05: Desarrollo de la metodología para el sistema

Fase 1: Inicio del Proyecto

Actividades del Product Owner:

1. **Definición de Requerimientos:**

   -Identificación de requisitos funcionales y no funcionales a partir de la descripción del sistema.

   -Creación de historias de usuario para cada funcionalidad mencionada.

2. **Priorización del Backlog:**

   -Clasificación de historias de usuario según su importancia y valor para los usuarios.

   -Establecimiento de prioridades en conjunto con el equipo de desarrollo.

Actividades del Scrum Master:

1. **Configuración del Entorno de Desarrollo:**

   -Coordinación con el equipo de desarrollo para configurar el entorno de desarrollo con las tecnologías mencionadas (Python, Django, HTML, JavaScript, SQL Server).

2. **Planificación del Sprint 1:**

   -Reuniones con el equipo para definir los objetivos y las historias de usuario a incluir en el primer sprint.

   -Establecimiento de un marco de tiempo para el sprint.

Actividades del Development Team:

1. **Setup del Proyecto:**

   -Creación de la estructura inicial del proyecto Django.

   -Configuración de la base de datos SQL Server.

   -Integración de las tecnologías frontend (HTML, JavaScript).

2. **Desarrollo del Módulo de Autenticación:**

   -Implementación del sistema de login.

   -Validación de credenciales y redirección según el tipo de usuario.

Fase 2: Desarrollo de Funcionalidades Principales

Actividades del Product Owner:

1. **Revisión del Sprint 1:**

   -Evaluación de las funcionalidades implementadas.

   -Feedback para ajustes y mejoras.

2. **Definición de Roles y Permisos:**

   -Especificación de roles (admin, user) y sus respectivos permisos.

-Creación de historias de usuario para la gestión de usuarios y permisos.

Actividades del Scrum Master:

1. **Planificación del Sprint 2:**
   -Selección de historias de usuario para el siguiente sprint.
   -Ajuste del backlog según la retroalimentación del Product Owner y el equipo.
2. **Revisión Continua del Código:**
   -Garantizar la calidad del código mediante revisiones continuas.

Actividades del Development Team:

1. **Implementación de Roles y Permisos:**
   -Desarrollo de la lógica para la gestión de roles y permisos.
   -Integración con el sistema de autenticación.
2. **Desarrollo de Módulos de Registro y Contrato**:
   -Creación de formularios y vistas para registrar la información del trabajador y sus contratos.

Fase 3: Desarrollo de Módulos Adicionales

Actividades del Product Owner:

1. **Revisión del Sprint 2:**
   -Validación de la implementación de roles y permisos.
   -Identificación de nuevas funcionalidades o ajustes.
2. **Definición de Funcionalidades de Programación de Roles:**
   -Especificación de historias de usuario para la programación de roles y horarios.

Actividades del Scrum Master:

1. **Planificación del Sprint 3:**
   -Selección de historias de usuario para el siguiente sprint.
   -Coordinación de recursos y dependencias.
2. **Gestión de Obstáculos:**
   -Identificación y resolución de obstáculos que puedan afectar el desarrollo.

Actividades del Development Team:

1. **Desarrollo de Módulo de Programación de Roles:**
   -Implementación de la lógica para la programación de roles y horarios.
   -Integración con la barra de visualización de horas programadas.
2. **Desarrollo de Módulo de Asistencia:**
   -Creación de vistas y consultas para visualizar las marcaciones y calcular los tiempos de asistencia.

Fase 4: Refinamiento y Pruebas

Actividades del Product Owner:

1. **Revisión del Sprint 3:**
   -Validación de las funcionalidades de programación de roles y asistencia.
   -Identificación de ajustes y nuevas funcionalidades.
2. **Definición de Funcionalidades de Cambio de Turno:**
   -Especificación de historias de usuario para el módulo de cambio de turnos.

Actividades del Scrum Master:

1. **Planificación del Sprint 4:**
   -Selección de historias de usuario para el siguiente sprint.
   -Coordinación de pruebas y revisión de código.
2. **Gestión de Retrospectivas:**
   -Organización de reuniones de retrospectiva para evaluar el desempeño del equipo y planificar mejoras.

Actividades del Development Team:

1. **Desarrollo de Módulo de Cambio de Turno:**
   -Implementación de la lógica para realizar cambios de turno.
   -Desarrollo de la interfaz de usuario para gestionar cambios de turno.

2. **Pruebas Unitarias y de Integración:**
   -Ejecución de pruebas para garantizar la calidad del código y la integración de módulos.

Fase 5: Implementación Final y Entrega

Actividades del Product Owner:

1. **Revisión del Sprint 4:**
   -Validación de todas las funcionalidades implementadas.
   -Aprobación para la entrega final.
1. **Definición de Funcionalidades de Justificación de Ausencias:**
   -Especificación de historias de usuario para el módulo de justificación de ausencias.

Actividades del Scrum Master:

1. **Planificación del Sprint 5:**
   -Últimas correcciones y mejoras según el feedback del Product Owner.
   -Coordinación de la preparación para la entrega final.
2. **Coordinación de Pruebas Finales:**

-Ejecución de pruebas finales y validación de la estabilidad del sistema.

Actividades del Development Team:

1. **Desarrollo de Módulo de Justificación de Ausencias:**
   -Implementación de la funcionalidad para justificar tardanzas o inasistencias.
   -Integración con el módulo de asistencia.
2. **Preparación para la Entrega:**
   -Aseguramiento de que toda la documentación esté lista.
   -Empaquetado y preparación para la implementación en el entorno de producción.

Entrega Final y Mantenimiento Continuo

Actividades del Product Owner:

1. **Aceptación del Producto:**
   -Confirmación de que el sistema cumple con los requisitos especificados.
   -Aprobación para su implementación en el entorno de producción.
2. **Planificación para Mantenimiento Continuo:**
   -Identificación de posibles mejoras y mantenimiento futuro.

Actividades del Scrum Master:

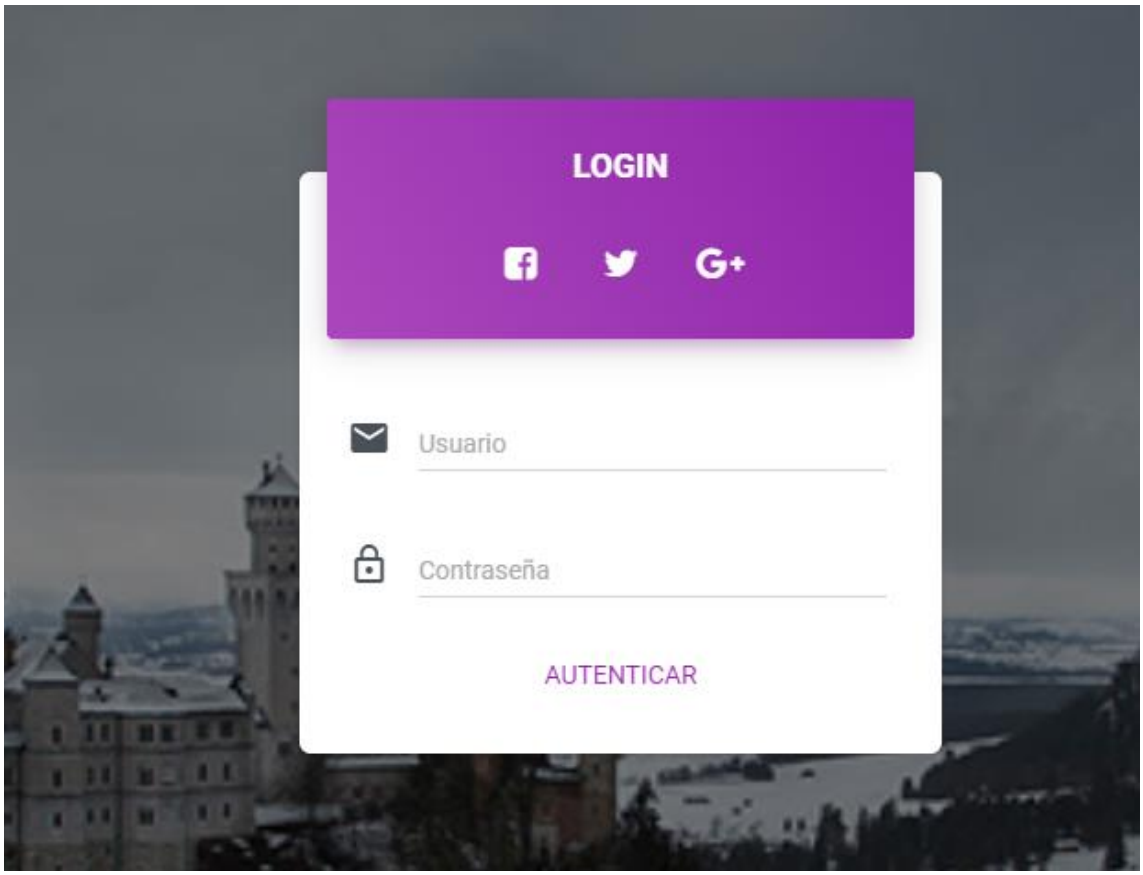
1. **Entrenamiento y Documentación:**
   -Capacitación del personal en el uso del sistema.
   -Documentación detallada para futuras referencias.
2. **Establecimiento de Métricas de Desempeño:**
   -Definición de métricas para evaluar el desempeño del sistema en producción.

Actividades del Development Team:

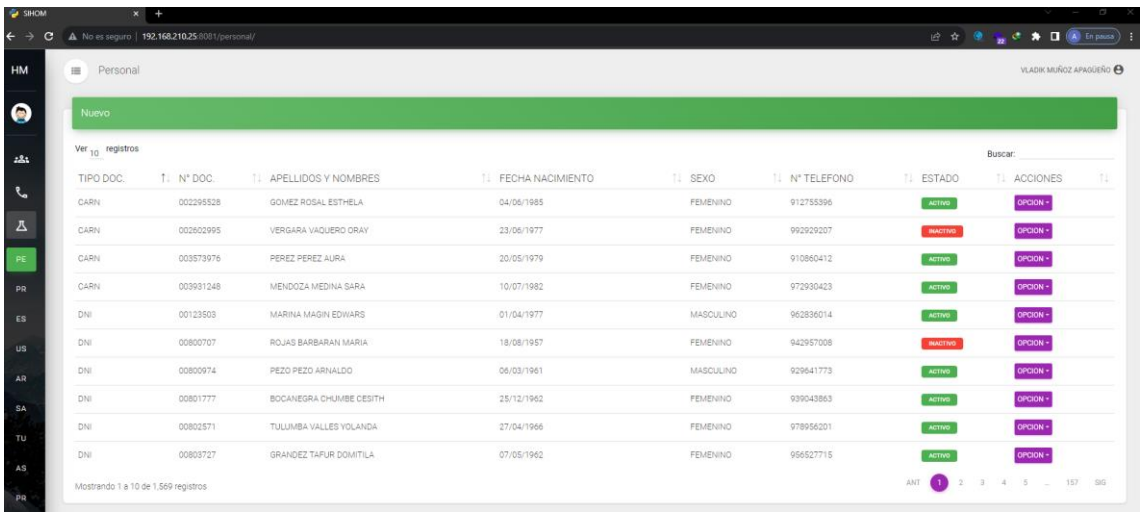
1. **Implementación en el Entorno de Producción:**
   -Despliegue del sistema en el entorno de producción.
   -Monitorización inicial para detectar posibles problemas.
2. **Soporte Inicial:**
   Disponibilidad para abordar problemas inmediatos tras la implementación.

Anexo 06: Prototipo del sistema

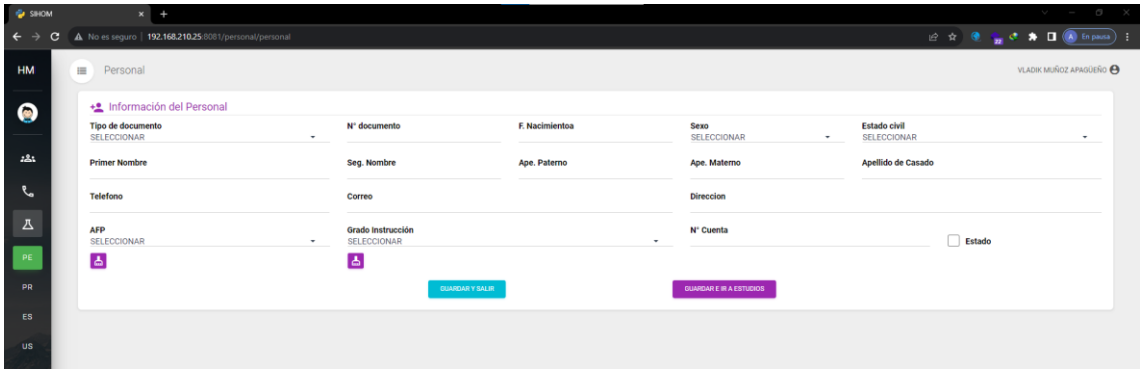
Vista de la autenticación



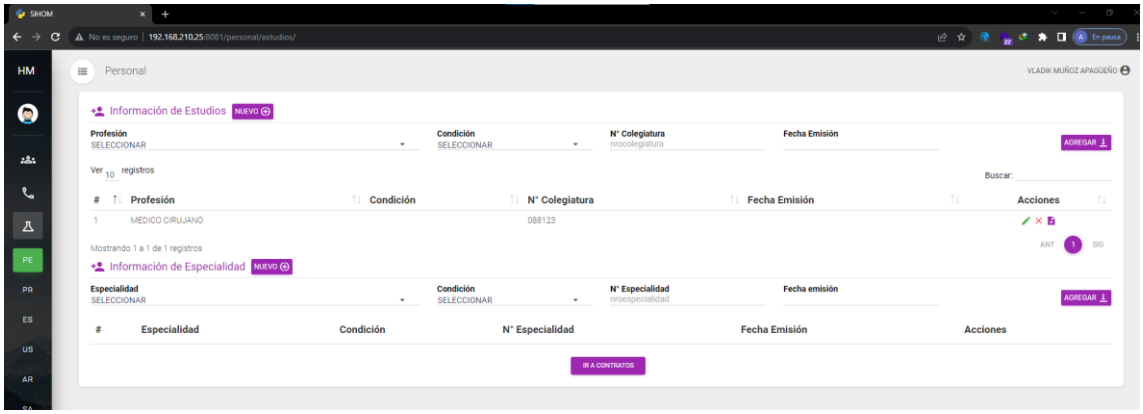
Lista del personal



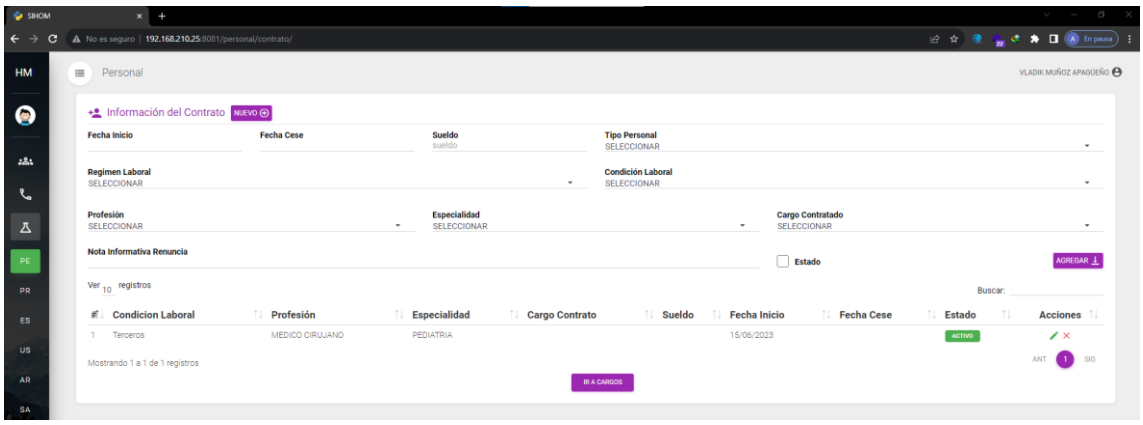
Modulo para registrar un nuevo personal



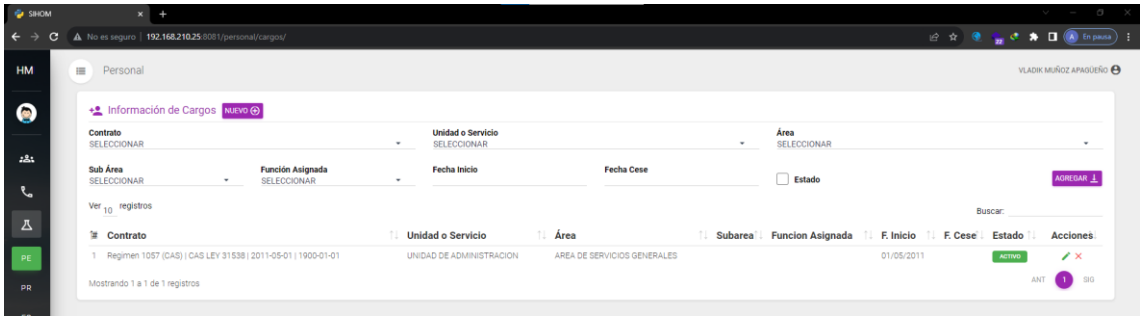
Apartado para registrar los estudios y especialidades del personal



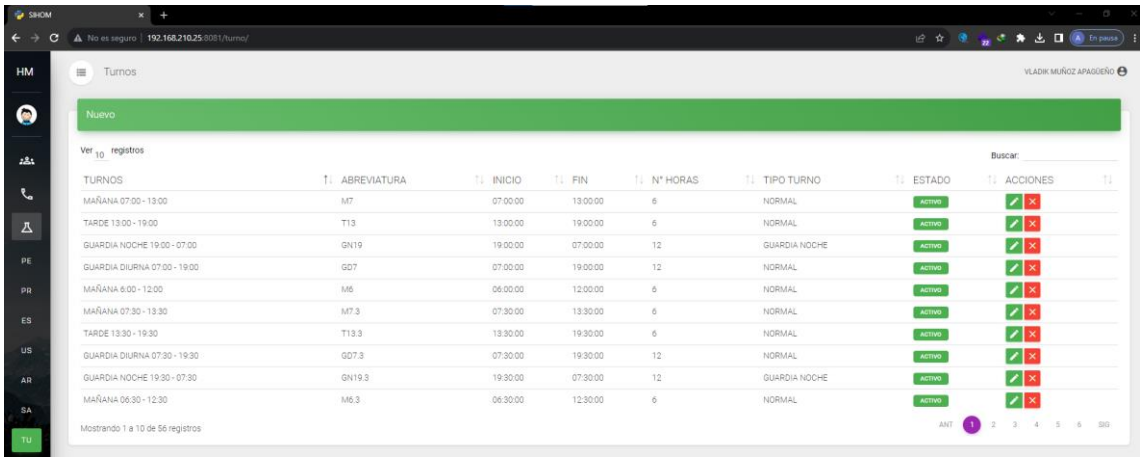
Registro del contrato del personal



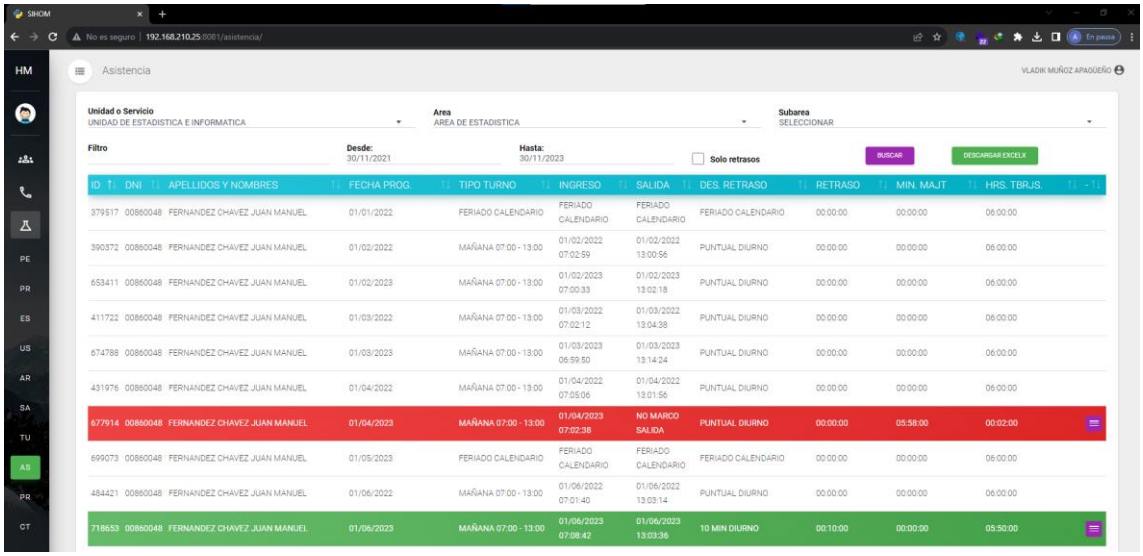
Información del cargo que tiene el personal



Lista de turnos para lo trabajadores

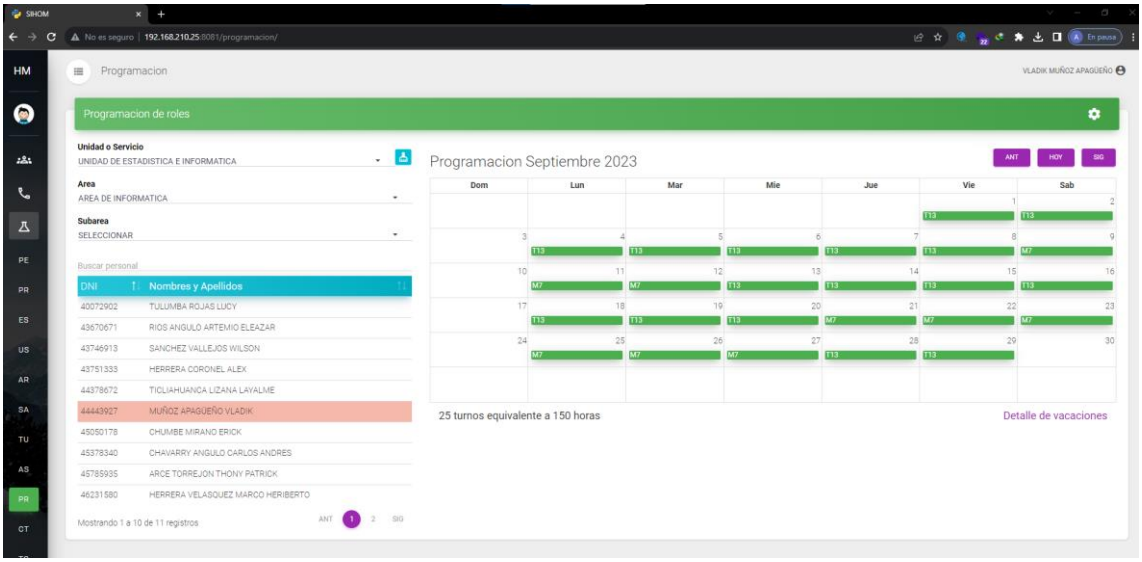


Módulo de asistencia

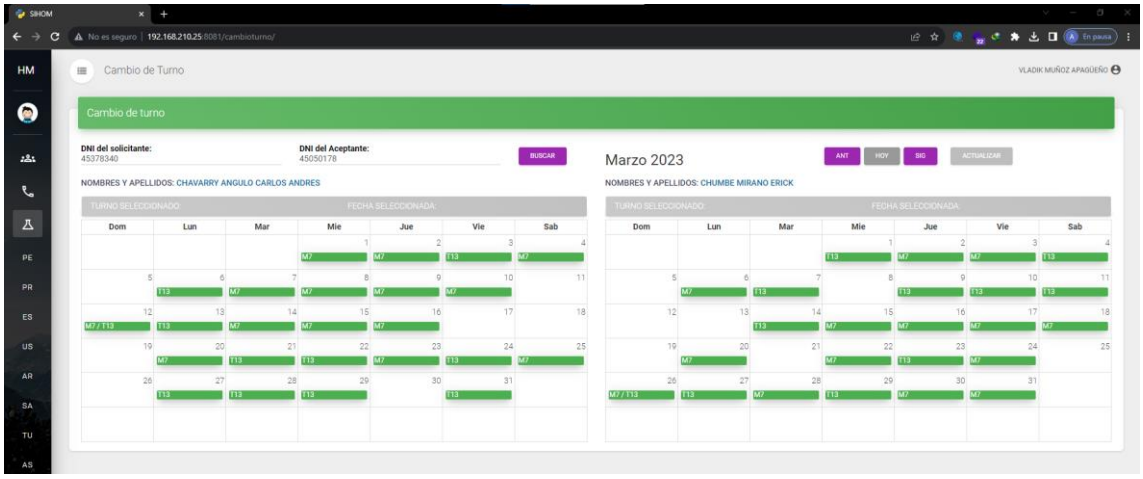


Venta modal para justificar una tardanza o inasistencia

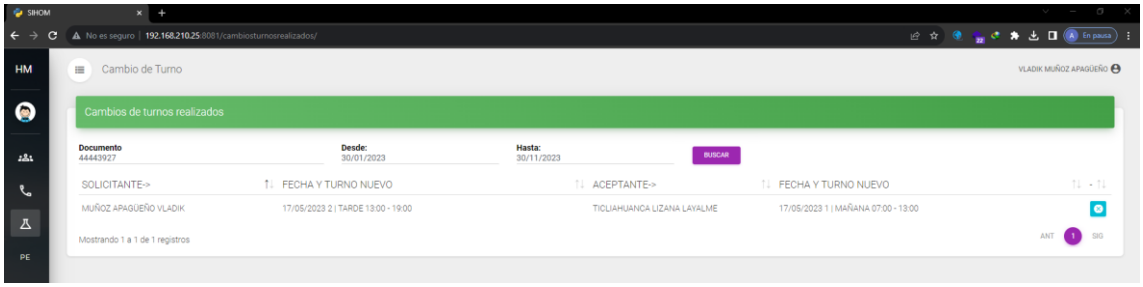
Modulo para realizar la programación de roles



Modulo para realizar los cambios de turnos entre trabajadores



Modulo para filtrar cambios de turnos como para anular



Anexo 07: Autorización de uso de información de Empresa

Solicitud Permiso para realizar trabajo de investigación

"AÑO DE LA UNIDAD, LA PAZ Y EL DESARROLLO"

ASUNTO: Solicito permiso para realizar Trabajo de Investigación

OGESS - ALTO MAYO
HOSPITAL II - 1 MOYOBAMBA
7:25
13 JUN 2023
MESA DE PARTES
HORA: FIRMA:

Dr. VARGAS EGAS VICENTE
Director del Hospital Moyobamba

Yo, Vladik Muñoz Apagüeño, identificado con DNI N° 44443927, con domicilio Jr. 20 de abril 545 Moyobamba. Ante usted respetuosamente me presente y expongo lo siguiente:

Que, estando cursando el noveno ciclo de la carrera profesional de ingeniería de sistemas en la universidad César Vallejo y actualmente realizando mis prácticas preprofesionales en el Hospital Moyobamba, solicito a Ud. permiso para realizar trabajo de investigación de recolección de datos como parte de mi proyecto de investigación.

Objetivo de la investigación: mi investigación tiene como objetivo desarrollar un "Sistema de control biométrico para la gestión de accesos de empleados" en el Hospital Moyobamba. Este sistema proporcionará una solución eficiente y segura para el registro y seguimiento de los accesos del personal, utilizando tecnologías biométricas.

Métodos de recolección de datos: para llevar a cabo esta investigación, utilizaré principalmente dos técnicas: la observación y la encuesta. La observación me permitirá recopilar información sobre los procesos de acceso existentes y analizar las necesidades y desafíos actuales. Además, implementaré una encuesta compuesta por 17 ítems, los cuales estarán estructurados mediante una escala de Likert.

Agradezco de antemano su consideración y apoyo en esta solicitud.

Moyobamba, 13 de junio del 2023

Atentamente;

.....
VLADIK MUÑOZ APAGÜEÑO
DNI Nº 44443927

AUTORIZACIÓN DE USO DE INFORMACIÓN DE EMPRESA

Yo Alexander Pérez Távara
(Nombre del representante legal o persona facultada en permitir el uso de datos)
identificado con DNI 41861445, en mi calidad de Jefe
(Nombre del puesto del representante legal o persona facultada en permitir el uso de datos)
del área de Unidad de Capacitación y Apoyo a la Docencia e Investigación
(Nombre del área de la empresa)
de la empresa Hospital II - 1 Moyobamba
(Nombre de la empresa)
con R.U.C N° 20531320060, ubicada en la ciudad de Moyobamba

OTORGO LA AUTORIZACIÓN,

Al señor(es) Wilson Díaz Bustamante - Vladik Muñoz Apagüeño,
(Nombre completo del o los estudiantes)
Identificado(s) con DNI N° 43238538 - 44443927 de la Carrera profesional de ingeniería de sistemas, para que utilice la siguiente información de la empresa:

Resultados de la Tesis titulada: Sistema de control biométrico para la gestión de accesos de empleados
(Detallar la información a entregar)

con la finalidad de que pueda desarrollar su ( ) Informe estadístico, ( )Trabajo de Investigación, (X) Tesis para optar el Título Profesional.

(X) Publique los resultados de la investigación en el repositorio institucional de la UCV.

Indicar si el Representante que autoriza la información de la empresa, solicita mantener en reserva el nombre o cualquier distintivo de la empresa, marcando con una "X" la opción seleccionada.

(X) Mantener en reserva el nombre o cualquier distintivo de la empresa; lo mencionaremos como "Hospital II - 1 Moyobamba".
( ) Mencionar el nombre de la empresa.

MINISTERIO DE SALUD
Perú Sanmartín
HOSPITAL II-1 MOYOBAMBA
Dr. Alexander Perez Tavara
JEFE DE LA UNIDAD DE CAPACITACION Y DOCENCIA
C.M.P. 53810 R.N.E. 82107

Firma y sello del Representante Legal

DNI:

El Estudiante declara que los datos emitidos en esta carta y en el Trabajo de Investigación, en la Tesis son auténticos. En caso de comprobarse la falsedad de datos, el Estudiante será sometido al inicio del procedimiento disciplinario correspondiente; asimismo, asumirá toda la responsabilidad ante posibles acciones legales que la empresa, otorgante de información, pueda ejecutar.

Wilson Díaz Bustamante
DNI: 43238538

Vladik Muñoz Apagüeño
DNI: 44443927

Moyobamba, 29 de diciembre de 2021

Señor (a):
DENNIS LEWIS PEREZ POSTIGO
Director
Hospital II-I Moyobamba

Atención:
Unidad de docencia y capacitación

Presente.-

Es grato dirigirme a usted para saludarlo, y a la vez manifestarle que dentro de mi formación académica en la experiencia curricular de investigación del X ciclo, se contempla la realización de una investigación con fines netamente académicos para la obtención de mi título profesional al finalizar mi carrera.

En tal sentido, considerando la relevancia de su organización, solicito amablemente su colaboración, para que pueda brindar la autorización de uso de información y publicación de su representada y obtener la información necesaria para la investigación titulada: "**Sistema de control biométrico para la gestión de accesos de empleados".** En dicha investigación me comprometo a mantener en reserva el nombre o cualquier distintivo de la empresa, salvo que se crea a bien su socialización.

Se adjunta la carta de autorización de uso de información y publicación, en caso que se considere la aceptación de esta solicitud para ser llenada por el representante de la empresa.

Así mismo se adjunta la carta, **"CARTA N° 020-2023-DIRESA-OGESS-AM/HII-1M/UCADel"**, donde se nos otorga la autorización para llevar a cabo el proyecto de investigación.

Del mismo modo se adjunta copia de documentos de identidad de los solicitantes.

Agradeciéndole anticipadamente por vuestro apoyo en favor de mi formación profesional, hago propicia la oportunidad para expresar las muestras de mi especial consideración.

Atentamente,

Wilson Diaz Bustamante
DNI: 43238538

Vladik Muñoz Apagüeño
DNI: 44443927