FECHA DE PRESENTACIÓN: 29 01 2025

DÍA MES AÑO

CARRERA: MECÁNICA INDUSTRIAL

APELLIDOS Y NOMBRES DEL ASESORADO:

CARRERA MORALES ALICIA MAGDALENA

APELLIDOS NOMBRES

TEMA DEL PROYECTO: IMPLEMENTACIÓN DE SISTEMAS DE CONTROL DE ACCESO BIOMÉTRICO PARA MEJORAR LA SEGURIDAD EN SIETE AULAS DE LA CARRERA DE MECÁNICA INDUSTRIAL DEL ISUCT

TUTOR: VICENTE ROMERO CARLOS JULIO

INFORME DE CUMPLIMIENTO :

	SI	NO
INFORME ESCRITO DE PROYECTO DE GRADO CULMINADO	X	

• SI SU RESPUESTA ES NO EXPLIQUE

	SI	NO
TRABAJO PRÁCTICO DE PROYECTO DE GRADO CULMINADO	X	

• SI SU RESPUESTA ES NO EXPLIQUE

	SI	NO
PROYECTO CUMPLE CON LOS OBJETIVOS PLANTEADOS EN EL PERFIL	X	

• SI SU RESPUESTA ES NO EXPLIQUE

	SI	NO
PROYECTO DE GRADO LISTO PARA REVISIÓN DEL TRIBUNAL	X	

- SI SU RESPUESTA ES NO EXPLIQUE

ADJUNTO REGISTRO DE SEGUIMIENTO DE ASESORÍA

NOMBRE Y FIRMA DEL DOCENTE:

12 02 2025

DÍA MES AÑO

FECHA DE ENTREGA DE INFORME

Visualizador de documentos

Turnitin Informe de Originalidad

Procesado el: 12-feb.-2025 2:25 p. m. -05
Identificador: 2586866637
Número de palabras: 12789
Entregado: 1

Sistemas Por Usuario User

Índice de similitud	Similitud según fuente	
10%	Internet Sources:	6%
	Publicaciones:	1%
	Trabajos del estudiante:	5%

13-02-2025
Aprobado

incluir citas | incluir bibliografía | excluyendo las coincidencias < 10 de las palabras | modo:
ver informe en vista quickview (vista clásica) | imprimir | actualizar | descargar

1% match (trabajos de los estudiantes desde 30-mar.-2017)
Submitted to Universidad Nacional de Colombia on 2017-03-30

1% match (trabajos de los estudiantes desde 21-ene.-2025)
Submitted to Universidad San Francisco de Quito on 2025-01-21

1% match ()
Santamaría Martínez, Jeny Carolina, Vargas Quintero, Leidy Viviana. "Propuesta solución integral de gestión de firma electrónica de documentos", Especialización en Gerencia y Tecnologías de Información, 2018

<1% match (Internet desde 18-dic.-2024)
https://WWW.coursehero.com/file/243935130/Introducci%C3%B3n-a-los-controles-de-Acceso-Biom%C3%A9tricodocx/

<1% match (Internet desde 09-nov.-2024)
https://WWW.coursehero.com/file/220577338/TAREA-3docx/

<1% match (Internet desde 15-dic.-2024)
https://WWW.coursehero.com/file/83988594/parte-5docx/

<1% match (Internet desde 06-dic.-2024)
https://WWW.coursehero.com/file/192072379/Entregable-2-planeaci%C3%B3n-avanzada-Mario-Figueroa-docx/

<1% match (Internet desde 19-dic.-2024)
https://www.coursehero.com/file/176581178/Reporte-de-servidores-HTTP-y-HTTPS-ADMINISTRACI%C3%93N-DE-REDESdocx/

<1% match (Internet desde 22-abr.-2024)
https://www.coursehero.com/file/230805269/EjerciciosSemana3doc/

<1% match (Internet desde 13-dic.-2024)
https://www.coursehero.com/file/243207850/La-IA-en-la-vida-cotidianadocx/

<1% match (trabajos de los estudiantes desde 23-ene.-2019)
Submitted to Universidad Internacional Isabel I de Castilla on 2019-01-23

<1% match (trabajos de los estudiantes desde 02-sept.-2019)
Submitted to Universidad Internacional Isabel I de Castilla on 2019-09-02

<1% match (trabajos de los estudiantes desde 03-dic.-2014)
Submitted to Universidad Internacional de la Rioja on 2014-12-03

<1% match (trabajos de los estudiantes desde 22-jul.-2021)
Submitted to Universidad Internacional de la Rioja on 2021-07-22

<1% match (Internet desde 16-ene.-2023)
https://www.slideshare.net/rizambrano/qua-tecnologas-biomtricas-aplicadas-ciberseguridadpptx

<1% match (Internet desde 21-ene.-2023)
https://www.slideshare.net/mejorlector/diseo-y-construccion-de-un-canal-hidraulico-de-pendiente-variable-para-uso-didactico-e-investigacion

<1% match (Internet desde 20-ene.-2023)
https://www.slideshare.net/GlendaColmenares1/teq-yuleidy-elena-herrera

<1% match (Internet desde 11-nov.-2020)
https://moam.info/table-of-contents_598241c21723dded563a4ec4.html

<1% match (Internet desde 04-may.-2023)
https://moam.info/university-of-trento-energy-efficient-medium-access_5c1b7efd097c4711588b465e.html

<1% match (trabajos de los estudiantes desde 28-ago.-2024)
Submitted to Corporación Universitaria Minuto de Dios,UNIMINUTO on 2024-08-28

<1% match ()
Arévalo González, Eugenio. "Reconocimiento automático de locutor en entornos forenses basado en técnicas de factor analysis aplicadas a nivel acústico", 2011

<1% match (Internet desde 22-mar.-2024)
https://appadvice.com/game/app/zendala/1600293805

<1% match (Internet desde 04-sept.-2023)
https://appadvice.com/game/app/solidario/1162832934

<1% match (trabajos de los estudiantes desde 04-nov.-2024)

Submitted to National University College - Online on 2024-11-04

<1% match (Internet desde 26-feb.-2022)
https://repository.unad.edu.co/jspui/handle/10596/31566?mode=full

<1% match (Internet desde 24-nov.-2020)
https://www.toodledo.com/tasks/public.php?f=0&h=0&id=td555bf29ed6849&s=4

<1% match (Joan Renard Meseguer. "Identification of genes related to seed longevity in Arabidopsis thaliana using genomic molecular techniques", Universitat Politecnica de Valencia, 2021)
Joan Renard Meseguer. "Identification of genes related to seed longevity in Arabidopsis thaliana using genomic molecular techniques", Universitat Politecnica de Valencia, 2021

<1% match (Internet desde 14-jun.-2020)
https://archive.org/stream/1.1FundamentosDeCircuitosElctricos5ta.EdicinSadiku/1.1%20Fundamentos%20de%20circuitos%20el%C3%A9c

<1% match (Internet desde 15-feb.-2006)
http://www.alternative-finance.org.uk

<1% match (trabajos de los estudiantes desde 20-sept.-2024)
Submitted to Instituto Tecnologico de Costa Rica on 2024-09-20

<1% match (Internet desde 25-ene.-2015)
http://www.arriolapartes.com.pe

<1% match (trabajos de los estudiantes desde 16-sept.-2007)
Submitted to Centro Escolar Entrevalles on 2007-09-16

<1% match (trabajos de los estudiantes desde 07-ene.-2025)
Submitted to ufidelitas on 2025-01-07

<1% match (trabajos de los estudiantes desde 12-may.-2024)
Submitted to Universidad Tecnológica Centroamericana UNITEC on 2024-05-12

<1% match (Internet desde 21-mar.-2024)
https://vdocumento.com/download/t4307-c278d.html

<1% match (trabajos de los estudiantes desde 02-oct.-2023)
Submitted to Corporación Universitaria Minuto de Dios, UNIMINUTO on 2023-10-02

<1% match (trabajos de los estudiantes desde 07-nov.-2024)
Submitted to UNAPEC on 2024-11-07

<1% match (trabajos de los estudiantes desde 09-jul.-2024)
Submitted to Universidad Argentina John F. Kennedy on 2024-07-09

<1% match (trabajos de los estudiantes desde 22-ene.-2024)
Submitted to Universidad Autónoma Metropolitana-Xochimilco on 2024-01-22

<1% match (trabajos de los estudiantes desde 28-abr.-2023)
Submitted to Universidad del Istmo de Panamá on 2023-04-28

<1% match (Internet desde 16-abr.-2024)
https://mtorial.com/la-inteligencia-artificial-oportunidades/

<1% match (trabajos de los estudiantes desde 12-may.-2024)
Submitted to Corporación Universitaria Iberoamericana on 2024-05-12

<1% match (trabajos de los estudiantes desde 10-sept.-2024)
Submitted to Universitat Politècnica de València on 2024-09-10

<1% match (Yauri, Rosa Magaly Sanes. "Factores que Afectan la Distribucion y Consumo de los Desayunos Escolares, del Programa Nacional de Alimentacion Escolar Qali Warma (Modalidad Raciones), en 15 Instituciones Educativas del Distrito de San Vicente de la Provincia de Canete.", Pontificia Universidad Catolica del Peru - CENTRUM Catolica (Peru), 2020)
Yauri, Rosa Magaly Sanes. "Factores que Afectan la Distribucion y Consumo de los Desayunos Escolares, del Programa Nacional de Alimentacion Escolar Qali Warma (Modalidad Raciones), en 15 Instituciones Educativas del Distrito de San Vicente de la Provincia de Canete.", Pontificia Universidad Catolica del Peru - CENTRUM Catolica (Peru), 2020

<1% match (Internet desde 24-may.-2024)
https://go.dormakaba.com/wes/articles/how-smart-building-technology-enhances-user-experience

<1% match (Internet desde 06-abr.-2024)
https://repositorio.uta.edu.ec/bitstream/123456789/39342/1/Tesis%20I.M.%20762%20-%20Tonato%20Palomo%20Denisse%20Anabel%20-%20Tutin%20Chicaiza%20Riquelme%20Estefania.pdf

<1% match (Internet desde 13-feb.-2024)
https://upc.aws.openrepository.com/bitstream/handle/10757/648670/Ter%c3%a1nV_C.pdf?isAllowed=y&sequence=17

<1% match (Internet desde 30-ene.-2008)
http://www.arabarri.net

<1% match (Internet desde 10-mar.-2022)
https://ddd.uab.cat/record/213423?ln=en

<1% match (Internet desde 14-nov.-2022)
https://digibuo.uniovi.es/dspace/bitstream/handle/10651/33761/TD_EliseoVi%c3%b1a.pdf?isAllowed=y&sequence=1

<1% match (Internet desde 23-abr.-2016)
http://media.proquest.com

<1% match (Internet desde 08-oct.-2022)
http://sedici.unlp.edu.ar

<1% match (Internet desde 08-jun.-2023)
https://www.panoramaaudiovisual.com/en/2022/01/31/haivision-logra-su-segundo-emmy-tecnico/

<1% match (Internet desde 02-nov.-2022)
https://www.udemy.com/course/crear-una-pagina-web-desde-cero-2020/

<1% match (Victoriya Lyashenko, Aleksey Muratov. "Modeling the risks process, associated with the violation of rolling stock operation", Revista Ingeniería UC, 2021)
Victoriya Lyashenko, Aleksey Muratov. "Modeling the risks process, associated with the violation of rolling stock operation", Revista Ingeniería UC, 2021

<1% match (Internet desde 14-abr.-2021)
https://doku.pub/documents/memoriastecnicaspdf-4qz3637wx90k

<1% match (Internet desde 28-nov.-2020)
https://eju.tv/2009/04/que-son-los-sistemas-biometricos/

<1% match (Internet desde 05-dic.-2020)
https://exonegocios.com/analisis-de-riesgo-que-es-definicion/

<1% match (Internet desde 08-ago.-2020)
https://mafiadoc.com/installation-instructions_599f13ef1723dd114090758b.html

<1% match (Internet desde 23-dic.-2022)
https://www.abebooks.com/9788466226660/D%C3%ADa-antig%C3%BCedad-Living-History-Life-8466226664/plp

<1% match (Internet desde 18-ene.-2007)
http://www.elcaminoacademy.com

Página 1 de 70 . PROYECTO DE INTEGRACIÓN CURRICULAR PROPUESTA TECNOLÓGICA Quito – Ecuador 2025 Página 1 de 70 . PROYECTO DE INTEGRACIÓN CURRICULAR PROPUESTA TECNOLÓGICA Quito – Ecuador 2025 Página 2 de 70 PROYECTO DE INTEGRACIÓN CURRICULAR - PROPUESTA TECNOLÓGICA CARRERA: MECÁNICA INDUSTRIAL TEMA: IMPLEMENTACIÓN DE SISTEMAS DE CONTROL DE ACCESO BIOMÉTRICO PARA MEJORAR LA SEGURIDAD EN SIETE AULAS DE LA CARRERA DE MECÁNICA INDUSTRIAL DEL ISUCT. Elaborado por: (Nombres y apellidos) Tutor: Carlos Julio Vicente Romero Fecha: 29 enero 2025 Página 3 de 70 . AGRADECIMIENTO A lo largo de este camino académico, he contado con el apoyo incondicional de muchas personas cuyos consejos, cariño y acompañamiento han sido fundamentales para cumplir esta meta. Agradezco, en primer lugar, a Alicia, mi madre, a mis hermanos: Sole, Elizabeth, Eduardo, a Diego por siempre estar ahí con una palabra, con su compañía, adaptándose a mis horarios, a mi hijo Mati; a ustedes por su amor incondicional. A mis amigos, quienes siempre me apoyaron con sus palabras de aliento, por creer en mí, en mis capacidades, su presencia ha sido un pilar sumamente importante. A mis compañeros, que jamás me hicieron sentir que estaba en una "carrera de hombres", su disposición para ayudarme fue de gran importancia en mi proceso de aprendizaje. Agradezco en especial a Christian, que siempre estuvo dispuesto a enseñarme, a explicarme, a intercambiar ideas y me brindó su amistad. A los buenos docentes, Diego B., por compartir sus conocimientos, por ser una guía y un ejemplo, por tener las ganas de enseñarnos más allá de lo requerido. A todos ustedes, gracias de corazón por ser parte de este logro, sin su presencia y apoyo seguramente hubiera sido un camino aún más difícil. Alicia Este logro no hubiera sido posible sin el apoyo incondicional de mi familia. Agradezco profundamente su paciencia, comprensión y aliento a lo largo de mi carrera. A mi hermana, la primera en creer en mí y en empujarme a dar ese primer paso. En especial, quiero expresar mi gratitud a mi madre, pilar fundamental en mi vida. Su constante motivación y ayuda fueron esenciales para culminar este trabajo. Su sacrificio y dedicación me inspiraron a perseverar. Gracias a ella, hoy puedo celebrar este triunfo. Espero que este logro sea un reflejo de todo lo que me ha enseñado. A mi compañera de tesis siempre valoraré tu amistad. Tus consejos han sido una guía en momentos difíciles. Gracias por tu sabiduría y apoyo incondicional. Nunca olvidaré tu generosidad y la confianza que depositaste en mí. Gracias por ser parte de mi historia y por creer en mí, incluso cuando yo mismo dudaba. Tu amistad es un regalo que atesoraré por siempre. Christian Página 4 de 70 DEDICATORIA A mi Mati, porque quiero ser un ejemplo y un camino a seguir para ti. A Diego, por ser mi mayor fortaleza y por enseñarme que los sueños se alcanzan con esfuerzo y dedicación. A mi familia y amigos, por su apoyo constante y por recordarme que nunca camino sola en este viaje. Y a todas las personas que creyeron en mí y me apoyaron. Alicia Este trabajo es el fruto de años de esfuerzo y dedicación, un logro que no habría sido posible sin el apoyo de mi gran amigo. Su ayuda constante durante cada obstáculo me brindó la fuerza para continuar. Ante cada desafío, su perspectiva y ánimo fueron esenciales. Lenin Pupiales, tu amistad y colaboración han sido fundamentales en este logro. Agradezco profundamente tu paciencia y dedicación a lo largo de este proceso. Tu contribución ha sido invaluable para la culminación de este trabajo. Por ello, dedico esta tesis a ti, con sincera gratitud y admiración. Christian Página 5 de 70 VALIDACIÓN Fecha: _____ Ing. Iván Choca _____ Ing. Carlos Vicente _____ Ing. Fernanda Galarza Página 6 de 70 APROBACIÓN DEL JURADO _____ Presidente (Nombres y apellidos) _____ Vocal 1 (Nombres y apellidos) _____ Vocal 2 (Nombres y apellidos) Página 7 de 70 . Índice de contenidos 1 CAPÍTULO I ..... 14 1.1 Formulación del Problema ..... 14 1.2 Objetivos ..... 14 1.2.1 Objetivo General ..... 14 1.2.2 Objetivos Específicos ..... 14 1.3 Justificación de la Propuesta Tecnológica ..... 15 1.4 Alcance..... 15 2 CAPÍTULO II ..... 16 2.1 Definición y Principios Básicos ..... 16 2.2 Origen de la Biometría..... 17 2.3 Características de las Tecnologías Biométricas ..... 18 2.4 Elementos de un Sistema Biométrico..... 18 2.5 Tecnologías Biométricas ..... 19 2.5.1 Modelo de las Tecnologías Biométricas ..... 19 2.6 Funcionamiento de un Sistema Biométrico ..... 23 2.7 Evaluación de Sistemas Biométricos..... 23 2.8 Tecnologías Biométricas Fisiológicas..... 24 2.8.1 Huella Dactilar..... 24 2.8.2 Reconocimiento Facial..... 25 2.8.3 Reconocimiento de Iris ..... 26 2.8.4 Reconocimiento de la Geometría de la Mano ..... 26 2.8.5 Reconocimiento de la Retina ..... 27 Página 8 de 70 . 2.8.6 Otras Formas de Biometría Fisiológica ..... 28 2.9 Usos y Aplicaciones de las Tecnologías Biométricas..... 29 2.10 Aplicaciones Actuales de las Tecnologías Biométricas ..... 30 2.11 Beneficios del Uso de Tecnologías Biométricas..... 32

ingresa y sale de las aulas. La carencia de un sistema integral de control de acceso ha generado preocupaciones sobre la seguridad de los recursos dentro de las aulas, afectando negativamente el ambiente de aprendizaje y el patrimonio de la institución. Este vacío en la seguridad se convierte en un riesgo potencial para la integridad de la comunidad académica y sus pertenencias. Por lo tanto, la necesidad apremiante de mejorar la seguridad en las aulas mediante la instalación de relojes biométricos con cerraduras electromagnéticas se presenta como una solución eficaz para mitigar los riesgos actuales y proporcionar un ambiente educativo más seguro y protegido. 1.2 Objetivos 1.2.1 Objetivo General Implementar un sistema de control de acceso biométrico con cerraduras electromagnéticas en las aulas de la Carrera de Mecánica Industrial del ISUCT con el propósito de fortalecer la seguridad, prevenir accesos no autorizados, y mejorar la gestión del control de ingreso a las instalaciones académicas para proporcionar un entorno educativo más seguro, eficiente y libre de riesgos, garantizando la protección de la comunidad académica y sus recursos. 1.2.2 Objetivos Específicos ? Ejecutar un diagnóstico previo de las aulas seleccionadas para determinar los accesos biométricos adecuados. Página 15 de 70 . ? Realizar una análisis comparativo de un control de acceso simple y un acceso biométrico. ? Realizar la instalación de los accesos biométricos en las siete aulas bajo normas de seguridad para su correcto funcionamiento. ? Realizar pruebas de funcionamiento de los controladores y accesorios. 1.3 Justificación de la Propuesta Tecnológica La implementación de un sistema de control de acceso biométrico con cerraduras electromagnéticas en las aulas de la Carrera de Mecánica Industrial del ISUCT se justifica ante la necesidad urgente de mejorar la seguridad en el entorno académico. La actual vulnerabilidad de las cerraduras convencionales y la pérdida frecuente de llaves han dado lugar a accesos no autorizados y actos de robo, por lo cual se presenta la urgencia de adoptar medidas más seguras. La introducción de tecnologías biométricas proporcionará un nivel adicional de seguridad al permitir una autenticación precisa de la identidad de los usuarios, eliminando así la posibilidad de acceso mediante llaves duplicadas o extraviadas. Además, la capacidad de registrar electrónicamente el acceso a las aulas facilitará un control administrativo más eficiente, permitiendo el monitoreo y la identificación de ingresos inusuales. Esta iniciativa busca no solo prevenir robos y accesos no autorizados, sino también contribuir a la creación de un ambiente educativo seguro y propicio para el aprendizaje. 1.4 Alcance Este proyecto se centra en la implementación de sistemas de acceso biométrico en siete aulas específicas de la Carrera de Mecánica Industrial del ISUCT proporcionando una solución integral y personalizada para fortalecer la seguridad, mejorando la gestión del control de ingreso a estas instalaciones. Con la instalación de los accesos biométricos, se contará con la seguridad necesaria en las aulas intervenidas, para crear un ambiente seguro y garantizando así el resguardo de los equipos y el mobiliario que se encuentran dentro de las mismas. Página 16 de 70 2 CAPÍTULO II FUNDAMENTACIÓN TEÓRICA 2.1 Definición y Principios Básicos La seguridad biométrica se define como el uso de características biológicas y conductuales que son exclusivas de cada individuo para llevar a cabo procesos de identificación y autenticación. Esta tecnología ha adquirido una importancia significativa en la actual era digital, donde la necesidad de sistemas de seguridad robustos es cada vez más evidente. En un mundo interconectado, donde las transacciones y la comunicación se realizan en línea, la protección de la información personal y sensible se ha vuelto crucial. La biometría ofrece una solución innovadora al proporcionar métodos de verificación que son difíciles de falsificar, como huellas dactilares, reconocimiento facial y escaneo de iris. A medida que la tecnología avanza, la seguridad biométrica se establece como un pilar fundamental para garantizar la integridad y la confidencialidad en diversas aplicaciones, desde el acceso a dispositivos móviles hasta sistemas de control de acceso en instalaciones sensibles. Definir de manera clara, toda la teoría (principios, leyes, conceptos) en los que se fundamenta la presente propuesta tecnológica. Como se muestra en la figura 1 los diferentes tipos de biometría. Figura 1. Biométrica Fuente: (Aviación al día, 2017) Página 17 de 70 2.2 Origen de la Biometría El término biometría tiene sus raíces en la antigua China, donde, hace más de mil años, los alfareros aplicaban sus huellas dactilares a los productos que creaban. Esta práctica no solo servía como un símbolo de distinción personal, sino que también funcionaba como una especie de firma, permitiendo a los artesanos diferenciar sus obras de las de otros. Este uso temprano de las huellas dactilares como medio de identificación refleja la búsqueda humana de formas únicas de reconocimiento y autenticidad. A medida que la historia avanzó, fue a comienzos de los años 70 cuando se desarrolló Identimat, un innovador sistema de identificación automática que se basaba en huellas dactilares. Este sistema fue diseñado específicamente para controlar el acceso físico a instalaciones, estableciendo así un precedente como la primera solución biométrica de uso comercial. La introducción de Identimat marcó un hito en la aplicación de la biometría, abriendo las puertas a nuevas posibilidades en la seguridad y la identificación. Desde entonces, la biometría ha experimentado un notable desarrollo, expandiéndose más allá de la simple identificación mediante huellas dactilares. Hoy en día, se reconocen y utilizan una variedad de rasgos biométricos, como el reconocimiento facial, el escaneo de iris y la identificación por voz, entre otros. Esta evolución refleja no solo el avance tecnológico, sino también la creciente necesidad de métodos de identificación más seguros y precisos en un mundo cada vez más digitalizado. La biometría se ha convertido en una herramienta esencial en diversas áreas, desde la seguridad pública hasta la protección de datos personales, consolidándose como un componente clave en la lucha contra el fraude y el acceso no autorizado. La alfarería fue el primer sistema de identificación por huellas dactilares como se puede observar en la Figura 2. Página 18 de 70 Figura 2. Alfarería y el primer registro de Huellas Dactilares Fuente: (Tesoro Guardados En Vasijas De Barro, 2022) 2.3 Características de las Tecnologías Biométricas Para que una característica, ya sea física o conductual, sea considerada un elemento válido de identificación, debe cumplir con ciertos requisitos. En primer lugar, debe ser universal, lo que significa que todos los individuos deben poseerla. En segundo lugar, debe ser singular, de modo que cada persona pueda ser identificada fácilmente a partir de sus características, ya que no existen dos individuos idénticos. Además, debe ser estable, lo que implica que la característica se mantenga constante a lo largo del tiempo y en diversas condiciones. También es necesario que sea cuantificable, es decir, que se pueda medir de manera objetiva. La característica debe ser aceptable, lo que se refiere al nivel de conformidad que el usuario tiene hacia ella. Asimismo, debe rendir, lo que implica que debe alcanzar un nivel de precisión suficiente para ser considerada confiable. Por último, no debe ser usurpar, lo que se refiere a la capacidad del sistema para resistir intentos de fraude. 2.4 Elementos de un Sistema Biométrico Un sistema biométrico se compone de varios elementos clave que permiten la identificación y autenticación de individuos a través de sus características únicas. Estos elementos son: ? Sensor: Este dispositivo es fundamental, ya que se encarga de captar los rasgos Página 19 de 70 . o características biométricas del individuo. El tipo de sensor utilizado dependerá de las características específicas que se deseen registrar y convertir en datos digitales. Por ejemplo, se pueden emplear sensores de huellas dactilares, cámaras para reconocimiento facial o escáneres de iris. ? Repositorio: Este componente se refiere a la base de datos donde se almacenan las plantillas biométricas registradas para su posterior comparación. Es crucial que esta base de datos esté protegida en un entorno físico seguro, además de ser cifrada y firmada digitalmente para garantizar la integridad y confidencialidad de la información almacenada. ? Algoritmos: Los algoritmos son el conjunto de códigos utilizados para procesar las características biométricas extraídas y realizar las comparaciones necesarias. Estos algoritmos son esenciales para asegurar que la identificación sea precisa y eficiente. 2.5 Tecnologías Biométricas Las tecnologías biométricas son métodos automáticos que permiten reconocer a las personas mediante sus rasgos físicos o de comportamiento. Entre los rasgos más comunes se encuentran la huella dactilar, el reconocimiento de voz, el iris del ojo y el reconocimiento facial. Dependiendo de la técnica biométrica empleada, se consideran diferentes parámetros para extraer un patrón de verificación único para cada individuo. 2.5.1 Modelo de las Tecnologías Biométricas Las tecnologías biométricas se estructuran en varios procesos fundamentales: ? Recopilación de Datos: Este proceso se encarga de la captación de datos biométricos y comienza cuando un usuario intenta acceder a un sistema controlado mediante técnicas biométricas. Los dispositivos encargados de esta captura son los sensores, que requieren que la información a captar sea lo más estandarizada posible. Sin embargo, el éxito de la captura también depende de características del dispositivo, como su calibración, calidad y sensibilidad. Página 20 de 70 . ? Transmisión de Datos: Este proceso generalmente se realiza en un lugar diferente al de almacenamiento. Las muestras biométricas suelen ocupar una cantidad considerable de espacio debido a la naturaleza de la información, como imágenes faciales o huellas dactilares. Para gestionar este volumen de datos, se utilizan dos enfoques: uno basado en sistemas de compresión estándar no necesariamente vinculados a datos biométricos, y otro que emplea algoritmos de cuantificación escalar para casos especiales. ? ? Procesamiento de Señales: La información obtenida de los procesos anteriores se trata mediante vectores de características, especialmente en el caso de huellas dactilares e imágenes faciales. Esta información se organiza y procesa en matrices para facilitar su análisis. Almacenamiento de Información: La información recopilada se almacena a

través de plantillas o patrones en una base de datos, utilizando tokens portátiles para asegurar su acceso. Posteriormente, se lleva a cabo el proceso de autenticación, donde se captura una muestra biométrica del individuo que se comparará con las plantillas previamente registradas. ? Proceso de autenticación: Que implica la captura de una muestra biométrica del individuo. Esta muestra será comparada con las plantillas previamente registradas en la base de datos. Este proceso puede realizarse de dos maneras distintas: identificación y verificación. o Identificación: En este método, se compara la muestra biométrica recogida del usuario con una base de datos que contiene rasgos biométricos registrados anteriormente. Lo interesante de este enfoque es que no requiere que el usuario proporcione información adicional, como su nombre o cualquier otro tipo de identificación. Esto se logra mediante cálculos complejos que permiten al sistema buscar coincidencias entre la muestra actual y cada uno de los registros almacenados. Así, la identificación se convierte en un proceso eficiente y rápido, que ayuda a garantizar la seguridad sin complicar la experiencia del usuario. o Verificación: En contraste, el proceso de verificación comienza con la Página 21 de 70 . identificación del usuario a través de algún método, como un ID, nombre de usuario, tarjeta o cualquier otro medio de reconocimiento. Una vez que se ha establecido la identidad del usuario, el sistema selecciona el patrón correspondiente en la base de datos que fue registrado previamente para esa persona. Este enfoque es particularmente útil en situaciones donde se requiere confirmar la identidad de un individuo específico, asegurando que solo aquellos autorizados puedan acceder a ciertos recursos o áreas. Posteriormente, el sistema biométrico recoge la característica biométrica del usuario y la compara con la que tiene almacenada en su base de datos. Este es un proceso relativamente sencillo, ya que solo implica la comparación de dos muestras, y el resultado se clasifica en positivo o negativo. Esta simplicidad permite que la autenticación sea rápida y eficiente, lo que es fundamental en situaciones donde el tiempo es un factor crítico. Las tecnologías biométricas se dividen principalmente en dos grupos, según la metodología utilizada: aquellas que analizan características fisiológicas, como huellas dactilares, iris o rasgos faciales, y aquellas que se centran en el comportamiento, como el reconocimiento de voz o patrones de escritura. Esta clasificación es importante porque cada tipo de tecnología tiene sus propias aplicaciones y niveles de efectividad. ? Toma de Decisión: El proceso de identificación y verificación culmina con la medición de un índice de comparación que se establece entre los patrones biométricos almacenados y los datos que el usuario ingresa al acceder al sistema. Este índice es crucial, ya que permite tomar decisiones sobre si la identificación y verificación son satisfactorias o no, garantizando así la seguridad del sistema. El proceso de toma de decisiones en biometría se descompone en cinco etapas clave: ? ? Búsqueda de Coincidencias: En esta fase, se realiza una comparación exhaustiva de las muestras biométricas para determinar el grado de similitud o correlación entre ellas. Esta comparación es esencial para identificar si la muestra capturada pertenece a un individuo específico. Cálculo de una Puntuación: Para llevar a cabo la comparación de datos biométricos, Página 22 de 70 . se calcula un valor numérico que indica el grado de similitud entre las muestras. Este valor se genera a partir de algoritmos avanzados que buscan coincidencias y producen una puntuación. Esta puntuación refleja la correlación entre la muestra que se desea autenticar y la que se encuentra registrada en la base de datos. ? Comparación con el Umbral Establecido: En el contexto de los sistemas biométricos, el término "umbral" se refiere a un valor predefinido por el administrador del sistema, el cual determina el grado de correlación necesario para que una muestra biométrica sea considerada similar a otra. Cuando la puntuación obtenida de la comparación entre muestras supera este umbral, se considera que las muestras son coincidentes. Es importante señalar que, aunque las muestras no sean idénticas, pueden ser consideradas similares debido a que el análisis tiene en cuenta posibles deficiencias en la captura de las muestras. Esto es crucial, ya que, en la práctica, las condiciones de captura pueden variar, y el sistema debe ser lo suficientemente flexible para adaptarse a estas variaciones. ? Toma de Decisión: La decisión final en un sistema biométrico es el resultado de la comparación entre la puntuación obtenida y el umbral establecido. Este proceso de decisión puede resultar en tres posibles salidas: coincidencia, no coincidencia e inconcluso. Una coincidencia puede permitir el acceso del usuario al sistema, mientras que una no coincidencia puede restringir dicho acceso. Por otro lado, si el resultado es inconcluso, significa que el sistema no ha podido determinar con certeza si la muestra obtenida corresponde a un registro existente, lo que puede llevar a solicitar al usuario que proporcione otra muestra. Este enfoque asegura que solo los individuos autorizados puedan acceder a recursos sensibles, manteniendo así la seguridad del sistema. ? Evaluación y Rendimiento: Los sistemas de evaluación y medición de rendimiento en tecnologías biométricas son fundamentales para establecer criterios objetivos que faciliten la comparación entre diferentes sistemas. Este tipo de evaluación puede ser un proceso costoso, ya que implica un análisis exhaustivo de datos, la extracción de conclusiones y la elaboración de la documentación pertinente. Además, se llevan a cabo pruebas de objetividad e independencia, que aseguran que los criterios Página 23 de 70 . utilizados sean válidos y robustos para el desarrollo de soluciones biométricas efectivas. 2.6 Funcionamiento de un Sistema Biométrico La fiabilidad y el funcionamiento de un sistema biométrico se pueden evaluar a través de una serie de tasas que reflejan su desempeño: ? Tasa de Error de Adquisición (Failure to Acquire Rate): Esta tasa indica el número de ocasiones en las que el sistema no puede capturar una muestra de calidad suficiente para su procesamiento. Un alto porcentaje en esta tasa puede señalar problemas en la tecnología de captura o en las condiciones ambientales. ? Tasa de Error de Registro (Failure to Enroll Rate): Se refiere a la proporción de la población que no puede generar muestras de calidad suficiente para ser almacenadas en el sistema. Esto puede ser un indicador de que ciertos individuos tienen características biométricas que el sistema no puede registrar adecuadamente. ? Tasa de Falso Negativo (False Rejection Rate): Esta tasa mide la frecuencia con la que el sistema no logra vincular a un individuo con su propia plantilla biométrica existente. Un alto porcentaje aquí puede resultar frustrante para los usuarios, ya que impide el acceso legítimo. ? Tasa de Falso Positivo (False Acceptance Rate): Se refiere a la proporción de ocasiones en las que el sistema erróneamente vincula a un individuo con la información biométrica de otra persona. Este tipo de error puede tener consecuencias graves, ya que podría permitir el acceso no autorizado a información sensible. 2.7 Evaluación de Sistemas Biométricos La evaluación de sistemas biométricos abarca una revisión exhaustiva de varios aspectos, desde la adquisición de datos hasta la integración del sistema en su totalidad. Entre los puntos más relevantes que se analizan se encuentran: ? Rendimiento en Funciones: Se evalúa la eficacia del sistema en el reconocimiento automático de personas. Página 24 de 70 . ? Seguridad, Integridad y Confidencialidad de los Datos: Es esencial garantizar que los datos biométricos se manejen de manera segura y confidencial, protegiendo la información personal de los usuarios. ? Fiabilidad y Mantenimiento del Sistema: Se considera la disponibilidad del sistema y la facilidad de su mantenimiento, aspectos críticos para su funcionamiento continuo. ? ? Comercialización y Costos: Se analiza la viabilidad del producto en el mercado, así como la estimación de costos y beneficios asociados. Aceptación por Parte del Usuario: La facilidad de uso y la aceptación del sistema por parte de los usuarios son factores determinantes para el éxito de cualquier tecnología biométrica. ? Aspecto Legal: Dado que los sistemas biométricos manejan información sensible, es vital considerar las implicaciones legales relacionadas con la seguridad y la privacidad de las personas. 2.8 Tecnologías Biométricas Fisiológicas 2.8.1 Huella Dactilar La huella dactilar es una característica morfológica única que se basa en la presencia de un conjunto de líneas genéricas, conocidas como crestas, y patrones de valles que se encuentran en la superficie de los dedos. Estas características se desarrollan durante los primeros meses del desarrollo fetal y permanecen constantes a lo largo de la vida, hasta que el cuerpo se descompone tras la muerte. Este rasgo es ampliamente utilizado en sistemas de identificación debido a su singularidad y facilidad de captura, convirtiéndose en uno de los métodos más comunes de verificación biométrica. “Finger Key”: Dispositivo usado para identificar operadores presionando el dedo, generando señales eléctricas como se muestra en la figura 3. Página 25 de 70 . Figura 3. Lectores Biométricos Fuentes: (Sistema de Control de Presencia, s.f.) 2.8.2 Reconocimiento Facial El reconocimiento facial es un mecanismo no intrusivo que permite identificar a una persona sin necesidad de contacto físico con un sensor. Junto con el reconocimiento de voz, es uno de los métodos más naturales que utilizan las personas para identificarse. Este sistema ha ganado una amplia aceptación en diversas aplicaciones, desde la seguridad hasta la interacción social, gracias a su conveniencia y la rapidez con la que puede llevarse a cabo. El sistema facial como herramienta clave para identificación, mediante el uso de algoritmos avanzados como se muestra en la figura 4. Figura 4. Sistema de Identificación Facial Fuente: (Buildeey , s.f.) Página 26 de 70 . 2.8.3 Reconocimiento de Iris El iris es la parte anular del ojo situada entre la pupila y la esclera, y su textura se forma durante el desarrollo fetal, estabilizándose en los primeros años de vida. La complejidad y riqueza de información que presenta el iris lo convierte en un rasgo biométrico altamente distintivo, ofreciendo un rendimiento excepcional en términos de identificación. Una de sus principales ventajas es que su captura no requiere contacto físico con el sensor. Sin embargo, existen desventajas, como su pequeño tamaño, que obliga al usuario a situarse a menos de

medio metro del dispositivo, y el costo elevado de los sensores. Además, factores como el uso de gafas o lentes de contacto pueden afectar la eficacia del sistema, y características físicas como las pestañas o los párpados pueden ocultar parte del iris, lo que es más común en ciertos grupos étnicos. Reconocimiento de iris para identificación biométrica, utilizando patrones únicos de iris para autenticar individuos como se muestra en la figura 5. Figura 5. Sistema de Identificación de Iris Fuente: (Williams Tancredi Comunicaciones S.A DE C.V, 2012) 2.8.4 Reconocimiento de la Geometría de la Mano El reconocimiento de la geometría de la mano se basa en diversas medidas, como la forma de la mano, el tamaño de la palma y las proporciones de los dedos. Este sistema presenta un costo bajo, ya que solo requiere fotografiar la mano, y es menos susceptible a factores como la humedad o la suciedad en comparación con la huella dactilar. Sin Página 27 de 70 . embargo, la capacidad de discriminación de la geometría de la mano no es tan alta, y puede variar a lo largo del crecimiento. Además, elementos como joyas, anillos o limitaciones de movilidad, como la artritis, pueden influir en la captura de la Figura. El tamaño del sensor también es considerable, ya que debe acomodar toda la mano, lo que puede generar preocupaciones de higiene entre los usuarios. Los sistemas modernos capturan la medida de los dedos, así como la estructura de la palma, lo que proporciona una huella única para cada individuo como se observa en la figura 6. Figura 6. Sistema de Reconocimiento por patrones de las manos Fuente: (TRIACINTER , 2022) 2.8.5 Reconocimiento de la Retina La retina, situada en la parte posterior del globo ocular, presenta un patrón de capilares que es único para cada individuo. Para capturar este patrón, se utilizan haces de luz infrarroja que atraviesan el cristalino, lo que requiere que el usuario coopere al situar su ojo a pocos centímetros del sensor. A pesar de la necesidad de esta cooperación, el reconocimiento retinal es considerado un método de alta seguridad, ya que es difícil de alterar o replicar. Su precisión y singularidad lo convierten en una opción valiosa para aplicaciones donde la seguridad es primordial como se observa en la figura 7. Página 28 de 70 . Figura 7. Sistema de Identificación de la Retina Fuente: (Penalva, 2006) 2.8.6 Otras Formas de Biometría Fisiológica ? Líneas de la Palma de la Mano: El reconocimiento de las líneas de la palma de la mano se basa en una serie de surcos y pliegues, similar a la técnica de huellas dactilares. Este método utiliza minucias para buscar coincidencias, aunque su uso actual se limita principalmente a investigaciones forenses. La singularidad de las líneas de la palma ofrece un potencial interesante, aunque todavía no se ha generalizado en aplicaciones comerciales. Como se observa en la figura 8 el sistema del sensor detecta al individuo. Figura 8. Sistema de Reconocimiento de líneas de la palma de la mano Fuentes: (Electronics Shop S.A, 2022) ? Estructura de las Venas de los Dedos o las Muñecas: Este sistema de reconocimiento se fundamenta en la compleja estructura de las venas en las Página 29 de 70 . manos o dedos, un rasgo que se define antes del nacimiento y que es diferente incluso en gemelos idénticos. Las propiedades más destacadas de este sistema incluyen su unicidad, universalidad y permanencia, además de que no requiere contacto físico al momento de la captura. La estructura venosa es inalterable, ya que se trata de un rasgo interno y complejo; sin embargo, el ejercicio intenso y ciertas condiciones de salud pueden provocar variaciones temporales en la apariencia de las venas. Se puede observar en la figura 9 como los escáneres infrarrojos capturan estos patrones con detalle permitiendo una autenticación precisa. Figura 9. Sistema de Identificación de Venas Fuente: (Kimaldi, 2020) 2.9 Usos y Aplicaciones de las Tecnologías Biométricas Las tecnologías biométricas han ganado un lugar destacado en el ámbito de la seguridad y la autenticación, siendo utilizadas tanto de manera independiente como en combinación con otros métodos de verificación. A diferencia de las contraseñas tradicionales, que requieren que los usuarios memoricen una serie de caracteres, las soluciones biométricas se basan en características únicas de cada individuo, como huellas dactilares, reconocimiento facial o patrones de voz. Esto significa que cada persona puede ser identificada de forma precisa y única, lo que minimiza el riesgo de errores y fraudes. Página 30 de 70 . Una de las principales ventajas de las tecnologías biométricas es su resistencia ante ciertos tipos de fraudes. Al utilizar datos que son inherentes a cada persona, como las características físicas o comportamentales, se dificulta notablemente la posibilidad de suplantación de identidad. Esto ha llevado a su adopción en una amplia variedad de sectores, desde la banca y las telecomunicaciones hasta la seguridad pública y el acceso a dispositivos electrónicos. Con el tiempo, el uso de estas tecnologías ha evolucionado y se ha expandido a diversas aplicaciones. Por ejemplo, en el ámbito financiero, muchas instituciones han implementado sistemas de autenticación biométrica para garantizar transacciones seguras. En el sector de la salud, se utilizan para proteger la información sensible de los pacientes, asegurando que solo el personal autorizado tenga acceso a datos críticos. Además, las tecnologías biométricas están comenzando a integrarse en la vida cotidiana de las personas. Desde el desbloqueo de teléfonos móviles hasta el acceso a edificios, su uso se está convirtiendo en algo común. Esta tendencia no solo mejora la seguridad, sino que también ofrece una experiencia más conveniente para los usuarios, eliminando la necesidad de recordar múltiples contraseñas y facilitando un acceso rápido y eficiente. 2.10 Aplicaciones Actuales de las Tecnologías Biométricas En la actualidad, las tecnologías biométricas se han integrado en una variedad de ámbitos, demostrando su versatilidad y eficacia. Varios estudios indican que su desarrollo y aplicación continúan avanzando, lo que sugiere un futuro prometedor para estas innovaciones en el campo de la seguridad y la autenticación. Entre las aplicaciones más destacadas de las tecnologías biométricas se encuentran: ? Control de acceso Físico y Lógico: Estas tecnologías permiten gestionar quién puede acceder a instalaciones físicas, como edificios y oficinas, así como a sistemas informáticos, garantizando que solo las personas autorizadas puedan ingresar. Página 31 de 70 . ? Control de Presencia: En entornos laborales, se utilizan sistemas biométricos para registrar la asistencia de los empleados, facilitando así la administración de recursos humanos y asegurando la puntualidad. ? Control de Fronteras: En aeropuertos y pasos fronterizos, las tecnologías biométricas ayudan a identificar a los viajeros de manera rápida y precisa, mejorando la seguridad y agilizando los procesos de verificación. ? Lucha Contra el Fraude: Estas soluciones son fundamentales para prevenir el uso indebido de identidades, especialmente en sectores como la banca y las finanzas, donde el riesgo de fraude es elevado. ? Investigación de Delitos: Las fuerzas del orden utilizan tecnologías biométricas para identificar sospechosos y resolver crímenes, analizando huellas dactilares y otros datos biométricos recogidos en escenas del crimen. ? Call-Center: En el ámbito de atención al cliente, las empresas están implementando sistemas de autenticación biométrica para verificar la identidad de los usuarios, mejorando la seguridad y la experiencia del cliente. ? Medio de Pago: Cada vez más, los consumidores utilizan métodos de pago biométricos, como el reconocimiento facial o las huellas dactilares, lo que no solo acelera las transacciones, sino que también las hace más seguras. ? Control Parental: Los padres pueden emplear tecnologías biométricas para supervisar y restringir el acceso de sus hijos a ciertos contenidos digitales, asegurando un entorno más seguro en línea. ? Vigilancia: En el ámbito de la seguridad pública, las cámaras equipadas con reconocimiento facial están siendo utilizadas para monitorear áreas públicas y detectar actividades sospechosas. ? Transacciones mediante Dispositivos móviles: La autenticación biométrica en smartphones se ha convertido en una norma, permitiendo a los usuarios realizar Página 32 de 70 . transacciones de manera rápida y segura, sin la necesidad de recordar contraseñas complejas. 2.11 Beneficios del Uso de Tecnologías Biométricas Las tecnologías biométricas ofrecen una amplia gama de beneficios tanto para las instituciones públicas y privadas como para los usuarios finales. Estas innovaciones están transformando la manera en que se gestionan los procesos de identificación y seguridad, convirtiéndose en una herramienta esencial en el mundo actual. 2.11.1 Para las Entidades Usuarias Las instituciones y organizaciones deben asumir el papel de líderes en la inversión y adopción de tecnologías biométricas, ya que los beneficios que se derivan de su implementación son significativos y variados. Entre las ventajas más destacadas, se encuentran: ? Aumento de la Seguridad: La biometría proporciona un nivel de seguridad superior al permitir la identificación única de las personas a través de características físicas, como huellas dactilares o reconocimiento facial. Esto reduce considerablemente el riesgo de acceso no autorizado. ? Reducción de Costes de Mantenimiento: Al implementar sistemas biométricos, las organizaciones pueden disminuir los gastos asociados con la gestión de contraseñas y otros métodos de identificación tradicionales, que requieren un mantenimiento constante. ? Aumento de la Eficiencia: Estas tecnologías permiten agilizar los procesos de verificación de identidad, lo que se traduce en un funcionamiento más rápido y eficiente de las operaciones diarias. ? Reducción del Fraude Interno: Al utilizar características biométricas únicas, se minimizan las posibilidades de fraude interno, ya que es mucho más difícil suplantar la identidad de una persona. Página 33 de 70 . ? Mejora de la Figura Corporativa: La adopción de tecnologías avanzadas como la biometría puede mejorar la percepción pública de una organización, proyectando una Figura de modernidad y compromiso con la seguridad. ? Oferta de Nuevos Servicios: La biometría abre la puerta a la creación de servicios innovadores que pueden mejorar la experiencia del usuario y ofrecer soluciones personalizadas. En la figura 10 se puede observar los problemas según la función. Figura 10. Definición de Problemas según la función Fuente: (Experto, 2001) En la figura 11 se puede observar la afectación según la función. Página 34 de 70 . Figura 11. Definición de Afectación según

el origen Fuente: (Gómez, 2015) 2.12 Riesgos El concepto de riesgo se refiere a la posibilidad de que una amenaza se materialice, es decir, que pase de ser una mera posibilidad a convertirse en una realidad. Esto ocurre cuando se aprovecha una vulnerabilidad dentro de un sistema de información. Es importante destacar que el riesgo solo existe en presencia de una amenaza y una vulnerabilidad; si falta alguno de estos elementos, el riesgo no tiene fundamento. En este sentido, el análisis de riesgos se convierte en una herramienta clave para la gestión de la seguridad, ya que permite identificar y evaluar las posibles amenazas que podrían afectar a un sistema. 2.13 Vulnerabilidades Las vulnerabilidades representan las probabilidades de que una amenaza se lleve a cabo contra un activo dentro de un sistema. La naturaleza de la vulnerabilidad depende del tipo de activo que se esté considerando; por ejemplo, un software puede tener vulnerabilidades específicas que lo hagan susceptible a ciertos tipos de ataques. La identificación de estas vulnerabilidades es fundamental para establecer medidas preventivas que protejan los activos y reduzcan la posibilidad de que las amenazas se materialicen. Página 35 de 70 2.14 Ataques Un ataque se define como la ejecución de una amenaza, ya sea de forma intencionada o accidental. Cuando una amenaza se concreta, se generan consecuencias que pueden variar en gravedad. Por ello, los ataques se clasifican en dos grupos principales como se observa en la tabla 1, aquellos que causan daños menores y aquellos que tienen un impacto significativo en la seguridad y funcionamiento del sistema. Esta clasificación permite a las organizaciones entender mejor los riesgos asociados y desarrollar estrategias efectivas para mitigar el impacto de posibles ataques, así como para mejorar la resiliencia de sus sistemas de información. Tabla 1. Clasificación de los ataques TIPOS DE ATAQUES ACTIVOS PASIVOS Cuando se producen alteraciones, Cuando solo se presentan accesos no eliminaciones, bloqueos o aumentos en autorizados al revisar información, pero la información del sistema. no existen daños significativos. Fuente: (Slideshare, 2006) 2.15 Proceso para el Análisis de Riesgos El análisis de riesgos es un proceso crucial que las organizaciones deben seguir antes de implementar cualquier medida de seguridad en sus sistemas de información. Este proceso implica una serie de pasos lógicos y sistemáticos que permiten identificar, evaluar y priorizar los riesgos asociados a las amenazas y vulnerabilidades existentes. A continuación, se presenta un esquema general que puede servir como guía: ? Identificación de Activos: Reconocer todos los activos dentro del sistema que podrían ser objeto de amenazas, como datos, hardware y software. ? Evaluación de Amenazas: Analizar las posibles amenazas que podrían afectar a estos activos, considerando tanto amenazas externas como internas. Página 36 de 70 . ? Identificación de Vulnerabilidades: Determinar las debilidades dentro del sistema que podrían ser explotadas por las amenazas identificadas. ? Análisis de Impactos: Evaluar las posibles consecuencias de que una amenaza se materialice, tanto en términos cuantitativos como cualitativos. ? Priorización de Riesgos: Clasificar los riesgos en función de su probabilidad de ocurrencia y el impacto que tendrían en la organización. ? Desarrollo de Estrategias de Mitigación: Diseñar e implementar medidas de seguridad adecuadas para reducir los riesgos a un nivel aceptable. ? Monitoreo y Revisión: Establecer un proceso continuo de monitoreo y revisión para garantizar que las medidas de seguridad sean efectivas y se ajusten a los cambios en el entorno de amenazas. Este enfoque sistemático no solo ayuda a proteger los activos de una organización, sino que también fomenta una cultura de seguridad que es fundamental en el entorno digital actual. La comprensión de este proceso permite a las empresas ser proactivas en la gestión de riesgos, asegurando así la integridad y la continuidad de sus operaciones. El análisis de seguimiento tiene su seguimiento como es visto en la Figura 12. Figura 12. Proceso de Análisis de Riesgo Fuente: (Blogger, 2015) Página 37 de 70 2.16 Control de Riesgos Una vez completado el análisis de riesgos, el siguiente paso consiste en identificar los servicios y medidas necesarias para garantizar la seguridad del sistema. Este proceso implica una evaluación cuidadosa de las herramientas y tecnologías que se requieren para proteger los activos de la organización. La determinación de estos servicios es fundamental, ya que permite establecer un entorno seguro que minimice las vulnerabilidades y proteja contra posibles amenazas. Así, se busca no solo cumplir con los estándares de seguridad, sino también crear un sistema robusto que pueda adaptarse a los desafíos cambiantes del entorno digital. 2.17 Modelos de Seguridad Los modelos de seguridad son representaciones formales que integran enfoques técnicos y matemáticos para establecer políticas de seguridad. Estas expresiones sirven como guías para evaluar y analizar los sistemas de información, proporcionando un marco estructurado que ayuda a las organizaciones a implementar medidas de protección efectivas. Al utilizar estos modelos, las empresas pueden identificar debilidades en sus sistemas y desarrollar estrategias adecuadas para fortalecer su seguridad, asegurando así la integridad y confidencialidad de la información que manejan. 2.18 Relación de la Biometría y la Seguridad En la actualidad, la biometría se ha convertido en una de las tecnologías más relevantes en el ámbito de la seguridad, utilizada principalmente para la identificación de usuarios. Por ejemplo, muchas instituciones financieras emplean sistemas biométricos para controlar el acceso a sus instalaciones y facilitar transacciones bancarias. Asimismo, en el comercio, los puntos de venta utilizan esta tecnología para validar compras mediante tarjetas de crédito, ofreciendo un nivel adicional de seguridad. Sin embargo, a pesar de sus ventajas, la biometría no está exenta de riesgos. Existen preocupaciones sobre la vulnerabilidad de estos sistemas, ya que la identificación biométrica puede ser objeto de fraudes o ataques. Por lo tanto, aunque la biometría Página 38 de 70 . representa una alternativa viable a las contraseñas tradicionales, es crucial que las organizaciones implementen medidas complementarias para proteger la información sensible de los usuarios. En este contexto, la biometría se presenta como una opción innovadora que, al ser utilizada de manera adecuada, puede mejorar significativamente la seguridad en diversas aplicaciones. Página 39 de 70 3. CAPITULO III DESARROLLO 3.1 Materiales En la Tabla 2 se puede determinar los materiales usados para la implementación del proyecto. Tabla 2. Implementación de Proyecto N° CANT. MATERIALES 1 7 2 7 3 7 4 7 5 7 6 7 7 7 8 7 9 100 10 1 11 1 12 3 13 1 14 1 15 5 16 2 17 1 18 1 19 50 20 2 21 1 Acceso biométrico con reporte de ingresos Cerraduras electromagnéticas de 280Kg Sensor de salida "No Touch" Fuente de poder de 2A, 12VDC con respaldo Batería de 7A, 12VDC Soporte Z para cerradura de 280Kg Soporte L para cerradura de 290Kg Cajas Dexon rectangulares Metro de cable UTP Cat. 5E Rollo de cable #14 Blanco Rollo de cable #14 Azul Cinta aislante negra (Tape) Caja de tornillos de Gypsun Caja de tornillos de madera Canaleta plástica Tuvería conduit 1m de termoretractil para cables Rollo de Alambre Galvanizado N18 Tacos para Gypsun Braker Caja cuadrada plastica de 20*20 Fuente: Propia Página 40 de 70 3.2 Métodos La investigación analítica desempeñará un papel crucial en la ejecución de este proyecto, ya que se utilizará para evaluar y comprender la situación actual del acceso a las aulas. Este análisis es esencial para tomar decisiones informadas, resolver problemas y seleccionar los equipos más adecuados según las necesidades identificadas. En primer lugar, se llevará a cabo un desglose exhaustivo de los desafíos de seguridad que se enfrentan, abarcando desde la pérdida de llaves hasta incidentes de hurto. Este proceso permitirá identificar variables clave que influirán en el éxito del sistema biométrico propuesto. A través de una revisión crítica de la literatura existente, se analizarán estudios y teorías relevantes que ayudarán a contextualizar el enfoque adoptado en este proyecto. Además, se realizará una comparación analítica de las alternativas tecnológicas disponibles, evaluando aspectos como la precisión biométrica, la adaptabilidad a diferentes entornos y los costos asociados. Esta evaluación permitirá determinar cuál opción se alinea mejor con los objetivos del proyecto. Posteriormente, se desarrollarán modelos conceptuales que facilitarán la visualización de la dinámica del sistema propuesto. Esto incluirá un análisis detallado de los costos en relación con los beneficios esperados, lo que permitirá tomar decisiones fundamentadas sobre la implementación del sistema. Durante y después de la implementación, se aplicará un enfoque analítico para evaluar los resultados obtenidos. Esto permitirá realizar ajustes continuos y garantizar que el sistema no solo cumpla con los estándares de seguridad, sino que también mejore su eficiencia operativa de manera constante. Así, se busca establecer un sistema robusto que asegure un entorno seguro y accesible para todos. Página 41 de 70 3.3 Diseño del proyecto 3.3.1 Sistemas de Seguridad Biométricos La seguridad en los entornos educativos es un aspecto fundamental para proteger la integridad de los recursos y asegurar un ambiente adecuado para el aprendizaje. En este contexto, la implementación de sistemas de control de acceso biométrico se presenta como una solución efectiva para fortalecer la seguridad. Estos sistemas abordan problemas comunes, como la pérdida frecuente de llaves y los incidentes de hurto en las aulas, que pueden afectar negativamente la experiencia educativa. Diversas investigaciones han puesto de manifiesto la eficacia de las tecnologías biométricas en la mejora de los procesos de autenticación y control de acceso. Al utilizar características únicas de los individuos, como huellas dactilares o reconocimiento facial, estos sistemas no solo incrementan la seguridad, sino que también facilitan el acceso a los espacios educativos, eliminando la necesidad de métodos tradicionales que pueden ser vulnerables. Además, la adopción de sistemas biométricos no solo beneficia a las instituciones educativas, sino que también crea un entorno más seguro para toda la comunidad académica. Este enfoque se ha convertido en uno de los métodos más utilizados a nivel mundial por diversas organizaciones, lo que subraya su

efectividad y confiabilidad. Al integrar estas tecnologías, las escuelas y universidades pueden garantizar un entorno donde los estudiantes y el personal se sientan protegidos, lo que a su vez fomenta un mejor clima de aprendizaje y desarrollo. 3.3.2 Reconocimiento Dactilar El reconocimiento dactilar, o dactiloscopia, ha recorrido un fascinante camino de evolución a lo largo de la historia, dividiéndose en tres etapas clave. En sus inicios, durante la prehistoria, los seres humanos utilizaban dibujos que servían como formas de identificación personal. Estos primeros intentos de marcar la individualidad sentaron las bases para el desarrollo posterior de esta práctica. Página 42 de 70 . La segunda etapa, conocida como la etapa empírica, se caracteriza por la capacidad de documentar huellas dactilares de manera sistemática. Durante este periodo, se comenzaron a registrar y analizar los patrones de las huellas, lo que permitió un entendimiento más profundo de su singularidad. Finalmente, la etapa científica ha revolucionado el campo mediante la incorporación de tecnologías biométricas avanzadas. En esta fase, se ha demostrado de manera concluyente que las huellas dactilares son únicas para cada individuo. Las rugosidades, los relieves y los surcos inter papilares forman un conjunto de características irrepetibles que distinguen a una persona de otra. Los patrones presentes en las huellas dactilares son tan específicos que no solo definen la identidad de cada individuo, sino que también permanecen inalterados con el paso del tiempo. Esta permanencia y singularidad proporcionan un alto nivel de seguridad, haciendo del reconocimiento dactilar una herramienta confiable en la autenticación y el control de acceso. Así, el uso de esta tecnología no solo refuerza la seguridad en diversos ámbitos, sino que también resalta la importancia de la identidad personal en un mundo cada vez más digitalizado. Como se observa en la figura 13 el escáner captura y compara todas las partes de la huella por lo cual este sistema es más preciso a la hora de identificación. Figura 13. Partes de la Huella Dactilar Fuentes: (Centro_certificador, 2024) Página 43 de 70 3.3.3 Estándares en Sistemas de Autenticación Biométrica ? Estándar ANSI 378 El estándar ANSI 378 es un pilar fundamental en el ámbito de la biometría, especialmente en lo que respecta a la autenticación mediante huellas dactilares. Este estándar fue creado para establecer un formato de intercambio de datos que asegure la estandarización en la representación de la información biométrica. Su importancia radica en que define de manera detallada cómo deben ser codificados y estructurados los datos biométricos, lo que es crucial para facilitar la interoperabilidad entre sistemas biométricos desarrollados por diferentes fabricantes. La interoperabilidad es esencial en un mundo donde se utilizan múltiples dispositivos y plataformas. Gracias al ANSI 378, los sistemas que cumplen con este estándar pueden comparar y autenticar huellas dactilares que han sido capturadas por diferentes dispositivos, independientemente de su origen. Esto no solo promueve la coherencia en el uso de datos biométricos, sino que también permite un flujo de información más eficiente y seguro entre distintos sistemas. Por ejemplo, en entornos de seguridad, como aeropuertos o edificios gubernamentales, la capacidad de autenticar identidades de manera rápida y precisa es vital para mantener la seguridad pública. Además, el uso de este estándar contribuye a reducir la posibilidad de errores y fraudes, ya que cada huella dactilar es única y su representación estandarizada minimiza el riesgo de confusiones. En resumen, el estándar ANSI 378 no solo mejora la seguridad, sino que también establece un marco confiable para la autenticación de identidad a través de huellas dactilares. ? Estándar ISO 19794-2 El estándar ISO/IEC 19794-2 se centra en el reconocimiento facial, estableciendo normas internacionales que regulan el intercambio de datos biométricos relacionados con esta tecnología. En un mundo cada vez más interconectado, donde la seguridad y la gestión de identidades son preocupaciones apremiantes, este estándar juega un papel crucial. Al Página 44 de 70 . definir un formato común para la representación de características biométricas faciales, facilita la interoperabilidad entre sistemas de reconocimiento facial de distintos fabricantes, permitiendo que diferentes tecnologías trabajen juntas de manera efectiva. Además de la interoperabilidad, el estándar ISO 19794-2 aborda aspectos críticos como los metadatos, la seguridad y la privacidad. Esto significa que no solo se centra en cómo se representan las características biométricas, sino también en cómo se gestionan y protegen esos datos. La seguridad de la información biométrica es de suma importancia, ya que cualquier brecha podría tener consecuencias graves para la privacidad de los individuos. Por lo tanto, este estándar garantiza que la captura, almacenamiento y transmisión de información biométrica se realice de manera segura y coherente. La implementación de este estándar tiene un impacto significativo en diversas aplicaciones, desde sistemas de seguridad en aeropuertos hasta plataformas de gestión de identidades en empresas. Al asegurar la consistencia y fiabilidad de los sistemas de reconocimiento facial, el ISO 19794-2 no solo mejora la seguridad, sino que también fomenta la confianza en el uso de tecnologías biométricas, lo que es esencial en un entorno donde la identidad digital se vuelve cada vez más relevante. ? Corriente Continua La corriente continua (DC) se define como un flujo constante de carga eléctrica que se desplaza en una única dirección. Este tipo de corriente es fundamental para el funcionamiento de muchos dispositivos electrónicos modernos, ya que permite un suministro estable y predecible de energía. A diferencia de la corriente alterna (AC), donde la dirección del flujo de electrones cambia periódicamente, la corriente continua proporciona un flujo constante que es ideal para dispositivos que requieren un voltaje estable. Muchos dispositivos electrónicos, como baterías, sensores, y chips de procesamiento, están diseñados para operar con corriente continua. Esto se debe a que la DC permite un funcionamiento más eficiente y fiable, lo que es especialmente importante en Página 45 de 70 . aplicaciones críticas donde la precisión es esencial. Por ejemplo, en dispositivos médicos, cualquier fluctuación en la corriente puede afectar su rendimiento y, por ende, la salud del paciente. Además, la corriente continua se utiliza ampliamente en sistemas de energía renovable, como paneles solares, donde la energía generada es en forma de DC y necesita ser gestionada adecuadamente para su uso. La importancia de la corriente continua va más allá de su función técnica; también representa un avance en la forma en que se gestionan y distribuyen las fuentes de energía modernas. ? Conexiones La terminal de control de acceso con huella digital de la serie DS-K1T8003EF es un dispositivo que combina tecnología avanzada con un diseño práctico. Equipado con una pantalla LCD de 2.4 pulgadas, este dispositivo no solo es funcional, sino también intuitivo, lo que facilita su uso en diversos entornos. Su capacidad para operar en modos de funcionamiento sin conexión y a través de red cableada (TCP/IP) lo convierte en una opción versátil para diferentes aplicaciones, desde oficinas hasta instalaciones de alta seguridad. Una de las características más destacadas de esta terminal es su funcionamiento con corriente continua. Esto permite la integración de un sistema de respaldo con baterías, asegurando que el dispositivo continúe operando incluso en caso de cortes de energía eléctrica. Esta capacidad de respaldo es crucial en situaciones donde la seguridad es primordial, ya que garantiza que el acceso a áreas restringidas permanezca controlado en todo momento. La combinación de tecnología biométrica avanzada, como el reconocimiento de huellas dactilares, con un diseño robusto y funcional, hace de la serie DS-K1T8003EF una solución ideal para instituciones que buscan mejorar su seguridad. En un mundo donde la protección de datos y la seguridad física son de suma importancia, este tipo de dispositivos se convierte en una herramienta esencial para la gestión de identidades y el Página 46 de 70 . control de acceso. Al ofrecer una solución confiable y eficiente, la terminal no solo mejora la seguridad, sino que también contribuye a un ambiente más seguro y protegido para todos. Como puede observar en la figura 14 las conexiones por grupos, numeración y características. Figura 14. Conexiones y Tecnología Fuente: (Manuales +, s.f.) Página 47 de 70 3.3.4 Principales elementos ? ACCESO BIOMÉTRICO: Es un dispositivo electrónico que permite la autenticación de los usuarios mediante huella o carnet (tarjeta RFID) para autorizar el ingreso a las aulas y que permite tener un reporte de las autenticaciones (ingresos) con fecha y hora exactas. ? CERRADURA ELECTROMAGNÉTICA: Es un dispositivo de seguridad que consta de una bobina dentro de un electroimán y un imán de alta potencia, cuando se energiza la bobina se genera un campo magnético fuerte que atrae y mantiene el imán en su lugar, bloqueando así la puerta. ? FUENTE DE PODER 12VDC: Una fuente de poder es un dispositivo eléctrico que mediante un transformados reduce los 110VAC que se obtiene de la red eléctrica a 16VAC, posteriormente un puente de diodos se encarga de rectificar el voltaje para obtener corriente continua de 12V que es el voltaje necesario para la cerradura y el control de acceso y asistencia biométrico. ? BATERÍA 12VDC: La batería utiliza la tecnología de plomo-ácido lo que permite acumular energía para que el sistema siga operativo en casos de cortes del suministro eléctrico, una de sus ventajas es que no requiere mantenimiento y es ideal para sistemas de seguridad. ? SENSOR NO TOUCH: Es un dispositivo que no requiere contacto, utiliza tecnología de proximidad (capacitiva) para detectar la presencia de un tejido como lo es una mano para accionar el relé interno que tiene y envía la señal para el control de acceso biométrico para cortar el flujo de corriente y desmagnetizar la cerradura, es ideal para este tipo de aplicaciones ya que al no tener contacto no se desgasta por el uso continuo. Página 48 de 70 . 3.4 Procedimiento general para la instalación de acceso biométrico con cerradura electromagnética sensor no touch. 3.4.1 Punto de conexión Como se muestra en la figura 15 se localizó el punto de conexión eléctrico más cercano de 110V, utilizando cable sólido #14 color azul para la fase y color blanco para el neutro. Figura 15. Puntos de conexión Fuente: Propia 3.4.2 Instalación de la

fuente. Se procede a instalar la fuente de energía que emite 12VDC y 2A requeridos para el sistema de control de acceso como se muestra en la figura 16. Figura 16. Instalación de fuente Fuente: Propia Página 49 de 70 . 3.4.3 Batería de respaldo Como muestra la figura 17 se instala la batería de respaldo que permite que el sistema funcione si existiera un corte de energía eléctrica. Figura 17. Batería de respaldo Fuente: Propia 3.4.4 Instalación de cerradura electromagnética Se determinó la ubicación exacta donde se instalaría la cerradura de acuerdo al marco de la puerta, figura 18. Figura 18. Ubicación de la cerradura Fuente: Propia Página 50 de 70 . Se marcó los puntos de fijación y posteriormente se perforó los orificios necesarios para la cerradura y para el imán como se ve en la figura 19. Figura 19. Puntos de fijación Fuente: Propia Se colocó chavetas en el imán para que quede totalmente fija y exista movimiento posteriormente debido al uso como se ve en la figura 20. Figura 20. Chavetas Fuente: Propia 3.4.5 Instalación del sensor no touch. Se seleccionó el lugar adecuado para el sensor no touch. Se marcó los puntos de montaje y se realizó las perforaciones necesarias. Se colocó una caja Dexon para tener una mejor estética en la instalación. Página 51 de 70 Figura 21. Instalación del sensor no touch Fuente: Propia 3.4.6 Instalación del módulo biométrico Se ubicó el dispositivo biométrico en una posición accesible para los usuarios y de acuerdo a la accesibilidad de las aulas. Se marcó los puntos de fijación y posteriormente se perforó los orificios necesarios. Se realizó la configuración inicial del módulo biométrico, registro de usuario administrador, fecha y hora, usuarios y tiempo de desbloqueo, como muestra la figura 22. Figura 22. Instalación del módulo biométrico Fuente: Propia 3.4.7 Verificación del Sistema Se realizaron pruebas del sistema completo simulando el uso normal del acceso y se realizaron los ajustes necesarios en el alineamiento de la cerradura, el sensor y el dispositivo biométrico. (Figura 23) Página 52 de 70 Figura 23. Verificación del sistema Fuente: Propia 3.4.8 Aulas instaladas Acceso Biométrico con Cerradura Electromagnética y Sensor No Touch Como se puede observar en las imágenes 24, 25, 26, 27,28,29, y 30 se encuentran instalados os sitemas de aceso biométrico. Figura 24. Aula CMI-07 Fuente: Propia Página 53 de 70 Figura 25. Aula CMI-08 Figura 26. Aula CMI-13 Fuente: Propia Fuente: Propia Página 54 de 70 Figura 27. Aula CMI-14 Figura 28. Aula CMI-15 Fuente: Propia Fuente: Propia Página 55 de 70 Figura 29. Aula Neumática Fuente: Propia Figura 30. Sala de docentes Fuente: Propia Página 56 de 70 4 CAPÍTULO IV ANÁLISIS DE RESULTADOS 4.1 Pruebas y resultados En el ámbito de la autenticación segura de usuarios, fue fundamental considerar diversos parámetros que guiaron la elección de un sistema específico según las necesidades particulares de cada situación. La selección de un sistema biométrico no puede ser arbitraria; debe basarse en una evaluación exhaustiva de indicadores que aseguren su eficacia y confiabilidad. Se identifica otros seis parámetros relevantes que también deben ser considerados en este tipo de evaluaciones: ? Seguridad ? Aceptación del Usuario ? Estabilidad ? Tiempo de Acceso ? Mantenimiento del Sistema Biométrico ? Universalidad ? Costo La implementación de sistemas de control de acceso biométrico en las aulas de la carrera de Mecánica Industrial del ISUCT tiene implicaciones significativas en varios aspectos clave. A continuación, se aborda cada uno de ellos de manera más extensa comparando el sistema tradicional manual con un sistema biométrico. 4.1.1 Seguridad ? Sistema Manual Los sistemas de control de acceso manual, tales como llaves o tarjetas, presentan múltiples vulnerabilidades. La posibilidad de perder una llave o que esta sea robada puede comprometer la seguridad del aula. Además, la duplicación de llaves es Página 57 de 70 . relativamente fácil, lo que puede permitir el acceso no autorizado. En situaciones donde se requiere que múltiples usuarios accedan a un espacio, el riesgo de que una llave caiga en manos equivocadas aumenta considerablemente. ? Sistema Biométrico Los sistemas biométricos, al utilizar características físicas únicas como huellas dactilares, reconocimiento facial o iris, ofrecen un nivel de seguridad superior. La probabilidad de que alguien pueda replicar estos rasgos es extremadamente baja. Además, estos sistemas pueden incluir tecnología de encriptación de datos, lo que añade una capa adicional de protección. En caso de un intento de acceso no autorizado, los sistemas pueden activar alarmas o notificaciones automáticas, lo que permite una respuesta rápida. 4.1.2 Aceptación del Usuario ? Sistema Manual La aceptación del usuario en sistemas manuales puede ser complicada. Muchos usuarios están acostumbrados a llevar llaves o tarjetas, pero esto no siempre es conveniente. La necesidad de recordar llevar estos objetos puede generar frustración. Además, si un usuario pierde su llave, puede causar inconvenientes significativos y requerir un proceso de reemplazo. ? Sistema Biométrico La aceptación de sistemas biométricos tiende a ser positiva, especialmente entre las generaciones más jóvenes que están familiarizadas con la tecnología. Aunque el proceso de registro inicial puede requerir tiempo, una vez que los usuarios están registrados, el acceso se vuelve mucho más eficiente. La comodidad de no tener que recordar una llave o tarjeta es un factor importante que mejora la experiencia del usuario. La capacitación y la comunicación sobre cómo funciona el sistema también son esenciales para aumentar la aceptación. Página 58 de 70 4.1.3 Estabilidad ? Sistema Manual Los sistemas manuales son propensos a fallos debido a factores humanos, como la pérdida de llaves o el desgaste de tarjetas. Estos problemas pueden causar interrupciones en el acceso, lo que resulta en pérdidas de tiempo y posibles frustraciones para los usuarios. Además, la dependencia de una persona para abrir el acceso puede llevar a situaciones en las que el aula esté cerrada sin previo aviso. ? Sistema Biométrico Los sistemas biométricos, aunque requieren un mantenimiento regular para asegurar su correcto funcionamiento, ofrecen una mayor estabilidad. Los problemas técnicos, como fallos en los sensores, son menos comunes y, cuando ocurren, pueden resolverse rápidamente con el soporte adecuado. La capacidad de estos sistemas para funcionar sin intervención humana directa reduce las posibilidades de errores y mejora la experiencia general del usuario. 4.1.4 Tiempo de Acceso ? Sistema Manual El tiempo de acceso en sistemas manuales puede ser considerable. En momentos de alta afluencia, como al inicio de clases, los estudiantes pueden verse obligados a esperar mientras buscan sus llaves o tarjetas. Esto no solo causa retrasos, sino que también puede generar aglomeraciones y desorganización. ? Sistema Biométrico Los sistemas biométricos permiten un acceso casi instantáneo. La identificación se realiza en segundos, lo que mejora la eficiencia en el flujo de entrada y salida de los estudiantes. Esto es especialmente beneficioso en entornos académicos, donde el tiempo es un recurso valioso. La rapidez del acceso también contribuye a una mejor Página 59 de 70 . experiencia general, ya que los estudiantes pueden concentrarse en sus actividades académicas sin distracciones innecesarias. 4.1.5 Mantenimiento del Sistema Biométrico ? Sistema Manual El mantenimiento de sistemas manuales es relativamente sencillo, pero puede ser costoso a largo plazo debido a la necesidad de reemplazar llaves o tarjetas perdidas. Además, la gestión de quién tiene acceso a qué puede convertirse en una tarea administrativa pesada. ? Sistema Biométrico Los sistemas biométricos requieren un enfoque más técnico para su mantenimiento. Esto incluye la calibración de los dispositivos de lectura y la actualización del software para asegurar que el sistema esté funcionando de manera óptima. Aunque el costo inicial de instalación puede ser alto, los beneficios a largo plazo, como la reducción de incidentes de seguridad y el ahorro en costos operativos, pueden justificar la inversión. La formación del personal de mantenimiento también es crucial para asegurar que el sistema funcione sin problemas. 4.1.6 Universalidad ? Sistema Manual Los sistemas manuales pueden ser limitados en su aplicación. Por ejemplo, si un estudiante olvida su tarjeta o pierde su llave, no podrá acceder al aula. Esto puede ser un inconveniente significativo en instituciones con un alto número de estudiantes, donde la diversidad de usuarios puede complicar aún más la gestión de accesos. ? Sistema Biométrico Los sistemas biométricos ofrecen una mayor universalidad, ya que pueden ser utilizados Página 60 de 70 . por cualquier persona que cumpla con los criterios de identificación. Esto es especialmente útil en entornos educativos, donde la diversidad de usuarios es alta. Además, los sistemas biométricos pueden integrarse con otras tecnologías, como sistemas de gestión estudiantil, lo que permite un acceso más fluido y eficiente. 4.1.7 Costo ? Sistema Manual Si bien los costos iniciales de un sistema manual pueden ser bajos, a largo plazo, los gastos relacionados con la seguridad, el reemplazo de llaves y la gestión de accesos pueden acumularse. Además, los costos ocultos, como el tiempo perdido debido a la ineficiencia, pueden ser significativos. ? Sistema Biométrico La implementación de un sistema biométrico puede requerir una inversión inicial considerable, pero los beneficios a largo plazo, como la reducción de incidentes de seguridad y el ahorro en costos de gestión, pueden justificar la inversión. Además, la mejora en la eficiencia operativa puede traducirse en un retorno sobre la inversión significativo. Es importante considerar no solo el costo inicial, sino también el valor que aporta en términos de seguridad y eficiencia. 4.1.8 Instrumentos y evaluación de Parámetros de Comparación Una vez que se han definido los parámetros de comparación, el siguiente paso consiste en evaluar y analizar la tecnología biométrica y la manual, lo que permitirá obtener una visión integral de los diferentes aspectos. Esto significa que se combinarán datos numéricos para ofrecer un panorama más completo y fundamentado. ? Análisis cuantitativo En este contexto, la tabla 3 presenta la evaluación realizada. Además, se incluye la sumatoria total de estos parámetros, lo cual facilita una comparación efectiva entre las diversas opciones estudiadas. Página 61 de 70 Tabla 3. Rubrica de Puntuación cuantitativa PARÁMETROS Dispositivos Dispositivos Manuales Biométricos. Seguridad 2 Aceptación del 2 Usuario Estabilidad Tiempo de Acceso Mantenimiento Universalidad Costo SUMATORIA 2 2 3 2 3 16 4 3

4 4 2 3 2 22 Fuente: Propia Notas de la valoración: Muy eficiente = 1 Deficiente = 2 Adecuado = 3 Excelente = 4 ? Análisis cualitativo Como se puede ver en la tabla 4 se hace una valoración cualitativa de ambos sistemas. Tabla 4. Rubrica de Puntuación cualitativa Parámetro Dispositivos Manuales Dispositivos Biométricos Seguridad Aceptación del Usuario Estabilidad Tiempo de Acceso Mantenimiento Universalidad Costo Vulnerables a pérdida y duplicación. Puede ser incómodo y frustrante. Propensos a errores humanos y fallos. Acceso lento, especialmente en horas pico. Sencillo, pero costoso a largo plazo. Limitados a usuarios con llaves o tarjetas. Bajo costo inicial, pero gastos ocultos. Alta seguridad, difícil de replicar. Generalmente bien aceptados, especialmente por jóvenes. Mayor estabilidad, menos intervención humana. Acceso rápido, mejora el flujo de usuarios. Requiere mantenimiento técnico regular. Accesible para todos los usuarios registrados. Alto costo inicial, pero ahorro a largo plazo. Fuente: Propia Página 62 de 70 4.1.9 Comparación ? Dispositivos manuales Tienen un rendimiento aceptable en mantenimiento y costo, pero son deficientes en seguridad, estabilidad y tiempo de acceso. ? Dispositivos biométricos Ofrecen alta seguridad y estabilidad, pero pueden ser más costosos y requieren mantenimiento técnico. 4.2 Conclusiones La integración de sistemas biométricos, como el reconocimiento de huellas dactilares o el escaneo facial, proporciona un nivel de seguridad superior al de los métodos tradicionales. Estos sistemas utilizan algoritmos avanzados de autenticación que analizan características únicas de cada individuo, lo que minimiza el riesgo de suplantación de identidad y acceso no autorizado. Además, al eliminar la necesidad de tarjetas de acceso, se reduce la posibilidad de pérdida o robo de identificaciones. Los sistemas biométricos están diseñados para ser intuitivos, lo que permite a los usuarios registrarse y acceder a las aulas con facilidad. La interfaz de usuario suele ser amigable, con instrucciones claras y procesos simplificados. Esto no solo mejora la experiencia del usuario, sino que también reduce el tiempo de espera en los puntos de acceso, optimizando el flujo de estudiantes y personal. Aunque la inversión inicial en tecnología biométrica puede ser considerable, los costos operativos a largo plazo se ven reducidos. La eliminación de la necesidad de emitir y reemplazar tarjetas de acceso, así como la disminución de incidentes de seguridad que pueden resultar en pérdidas económicas, contribuyen a un retorno de inversión positivo. Además, los sistemas biométricos requieren menos mantenimiento en comparación con sistemas de acceso tradicionales. Página 63 de 70 . Los sistemas biométricos permiten la recopilación automática de datos de asistencia, lo que se traduce en una gestión más eficiente. Los datos se almacenan en bases de datos seguras y pueden ser analizados para generar informes sobre patrones de asistencia, facilitando la toma de decisiones administrativas. Esto también mejora la precisión, ya que se eliminan errores humanos asociados con el registro manual. Los sistemas de control de acceso biométrico son altamente adaptables, permitiendo la integración con otras tecnologías de seguridad, como cámaras de vigilancia y sistemas de alarma. Además, pueden escalarse fácilmente para incluir nuevas aulas o áreas, lo que proporciona flexibilidad a medida que crecen las necesidades de la institución. Esto asegura que la inversión en tecnología siga siendo relevante y útil a largo plazo. La adopción de sistemas biométricos en lugar de chapas tradicionales representa una oportunidad valiosa para avanzar hacia un futuro más sostenible. Al reducir la dependencia de materiales físicos, mejorar la seguridad y fomentar el uso eficiente de los recursos, estas tecnologías no solo benefician a los usuarios en términos de comodidad y protección, sino que también contribuyen significativamente a la conservación del medio ambiente. En este sentido, la biometría se presenta como una solución innovadora que alinea la seguridad personal con la responsabilidad ecológica, promoviendo un entorno más seguro y saludable para todos. 4.3 Recomendaciones Es fundamental implementar un programa de capacitación que incluya tanto sesiones teóricas como prácticas sobre el uso de los sistemas biométricos. Esto debe abarcar desde la operación básica hasta la solución de problemas comunes. Incluir guías y tutoriales en línea puede facilitar el acceso a la información. La capacitación continua asegurará que todos los usuarios se sientan cómodos y competentes al utilizar la tecnología. Se debe establecer un cronograma de mantenimiento preventivo que incluya revisiones periódicas de hardware y software. Esto puede incluir la limpieza de los dispositivos de escaneo, actualizaciones de firmware y pruebas de funcionalidad. Además, es Página 64 de 70 . recomendable contar con un servicio técnico especializado que pueda atender cualquier problema de manera rápida y eficiente, minimizando el tiempo de inactividad. Realizar evaluaciones semestrales o anuales del sistema permitirá identificar áreas de mejora y oportunidades para la actualización tecnológica. Esto incluye la revisión de las capacidades del software, la evaluación de la satisfacción del usuario y la consideración de nuevas tecnologías emergentes en el campo de la biometría. Mantenerse al día con las tendencias del mercado garantiza que la institución no solo mantenga la seguridad, sino que también aproveche las innovaciones que mejoren la eficiencia del sistema. 5 Bibliografía Aviación al día. (2 de Junio de 2017). Aviación al día. Obtenido de https://aviacionaldia.com/2017/06/jetblue-y-delta-probaran-abordajes-usando- tecnologias-biometricas.html Blogger. (31 de Mayo de 2015). Obtenido de https://angelwalle.blogspot.com/2015/05/25- analisis-de-riesgo-dentro-del-sgsi.html Buildeey . (s.f.). Obtenido de https://buildeey.com/profile/sefa-security-systems-llc Centro_certificador. (1 de Agosto de 2024). Instagram. Obtenido de https://www.instagram.com/centro_certificador/p/C-JRya0Kpnw/?img_index=2 Electronics Shop S.A. (2022). Eshopgroup. Obtenido https://www.eshopgroup.com/?/productos/acceso_peatonal/2424 Experto. (7 de Marzo de 2001). Gestiopolis. Obtenido https://www.gestiopolis.com/administrador-que-es-que-hace-habilidades- competencias/ Gómez, C. (15 de Febrero de 2015). Issuu. Obtenido https://issuu.com/creacionesvisionarias/docs/mdetel_comdetel751095.docx Kimaldi. (20 de Enero de 2020). Obtenido de de de de Página 65 de 70 https://www.kimaldi.com/aplicaciones/biometria_vascular/utilizar-sistemas- biometricos-para-conseguir-el-balance-perfecto-entre-seguridad-y-usabilidad/ Manuales +. (s.f.). Obtenido de https://manuals.plus/es/hikvision/secure-door-control- unit-ds-k2m061-manual Penalva, J. (23 de Mayo de 2006). Xataka. Obtenido de https://www.xataka.com/otros/jiris-ofrece-seguridad-biometrica-a-traves-de-una- webcam Sistema de Control de Presencia. (s.f.). Riyac 9V. Obtenido de https://www.sistemacontrolpresencia.com/es/home/46-lector-de-huellas-de-sobremesa-hamster.html Slideshare. (2006). Modelo para la selección de software ERP. Obtenido de https://es.slideshare.net/slideshow/factores-de-riesgo-biologico- 1351947/1351947 Tesoro Guardados En Vasijas De Barro. (27 de Septiembre de 2022). Facebook. Obtenido de https://aviacionaldia.com/2017/06/jetblue-y-delta-probaran-abordajes-usando-tecnologias-biometricas.html TRIACINTER . (2022). Obtenido de https://www.triacinter.com/producto/lector-scanner- de-mano-biometrico-handpunch-2000-schlage/ Williams Tancredi Comunicaciones S.A DE C.V. (27 de Junio de 2012). Slideshare. Obtenido de https://es.slideshare.net/slideshow/catalogo-soluciones-williams- tancredi/13476682#15 Página 66 de 70 6. Anexos Se anexa las facturas correspondientes. Página 67 de 70 Página 68 de 70 Página 69 de 70 Página 70 de 70 . . . . . .