



Diseño de un prototipo funcional de un sistema de Autenticación Biométrica basado en Reconocimiento facial para el acceso a SAP en la universidad EAN

Presentado por:

Santiago Marín Patiño

Santiago Patiño Carreño

Gisell Zamudio García

Director (a):

Figueroa Hernández Diana Paola

Universidad EAN



Diseño de prototipo funcional de un sistema de Autenticación Biométrica basado en Reconocimiento facial para el acceso a SAP en la universidad EAN

Presentado por:

Santiago Marín Patiño

Santiago Patiño Carreño

Gisell Zamudio García

Trabajo de grado presentado como requisito de grado para optar el título de:

Ingeniero de Sistemas

Director (a):

Figueroa Hernández Diana Paola

Universidad EAN

Facultad de Ingeniería

Programa Ingeniería de Sistemas

Bogotá, Colombia

28/02/2026

Nota de aceptación:

Firma del jurado

Firma del jurado

Firma del director del trabajo de grado

Ciudad, día/mes/año

Índice

Resumen Ejecutivo	5
Abstract	6
Introducción	7
Pregunta de investigación	9
Objetivos	10
Definición del problema	11
Justificación	12
Marco Teórico	13
Estado del arte (Metodología Prisma)	24
Metodología	29
Resultados y Análisis	36
Discusión	46
Plan de Divulgación	52
Conclusiones	54
Referencias	56

Resumen Ejecutivo

El uso de la plataforma SAP permite gestionar procesos administrativos. Sin embargo, existen desafíos que se experimentan en repetidas ocasiones e incluso en momentos críticos para los estudiantes, como lo es la gestión de la contraseña en SAP. Este sistema de gestión, que es fundamental para acceder a notas, hacer la inscripción a materias, consultar los horarios, hacer pagos en línea, descargar y solicitar certificados, hacer solicitud de aplazamientos y hacer actualización de datos personales, exige actualizar la clave periódicamente. Esto convierte la experiencia de los estudiantes en procesos repetitivos, molestos y en muchos casos estresantes, especialmente cuando se deben manejar múltiples contraseñas para diferentes plataformas institucionales.

Teniendo en cuenta esta problemática en específico, se plantea la necesidad de hacer una investigación para buscar soluciones que permitan hacer este proceso de autenticación en SAP más ágil y accesible. Luego de revisar diferentes alternativas tecnológicas y analizar su viabilidad en el entorno universitario, se identificó que la autenticación biométrica, particularmente mediante reconocimiento facial, podría brindar a los estudiantes una experiencia mucho más eficiente.

Apoyado de la recolección de 97 perspectivas de los estudiantes de la EAN mediante una encuesta, se propone desarrollar un prototipo funcional de un sistema de autenticación biométrica orientado a facilitar el acceso a la plataforma SAP como alternativa al modelo tradicional de acceso por contraseña. Para el desarrollo del proyecto se adoptó un enfoque

metodológico mixto, que combinó la recolección de información mediante encuestas dirigidas a los estudiantes de la universidad EAN, el análisis de su percepción frente al mecanismo actual de autenticación y el desarrollo de un prototipo funcional utilizando el lenguaje de programación Python con diferentes librerías especializadas como “face_recognition”.

Los resultados obtenidos muestran que los estudiantes presentan con gran frecuencia inconvenientes con la gestión de contraseñas y una percepción favorable frente al uso de tecnologías de autenticación biométrica como alternativa al acceso. Esta solución no solamente busca simplificar el proceso de autenticación, sino también aportar mayor facilidad de acceso, seguridad y adopción de nuevas tecnologías además de mejorar la experiencia digital de la comunidad estudiantil de la EAN.

Palabras clave: Autenticación Biométrica, Reconocimiento facial, Autenticación Multifactor, Ciberseguridad; Sistemas ERP; Experiencia de usuario; Educación Superior.

Abstract

The university environment presents various challenges related to the management of institutional digital services. Among these, one of the most recurrent issues is the management of access credentials to the SAP system, which is essential for accessing academic information, services, and administrative processes. This system requires periodic password updates, making access a repetitive, inefficient, and often stressful process for students, especially when multiple platforms require independent authentication.

In this context, the present study aimed to analyze technological alternatives to optimize the authentication process and improve user experience. To achieve this, a mixed-methods approach was adopted, including the application of surveys to students to identify perceptions and difficulties associated with system usage, the development of a functional prototype based on facial recognition, and the analysis of user acceptance of this technology as an access mechanism.

The results show that a significant proportion of students perceive password management as problematic and impractical. Additionally, the developed prototype proved to be a viable alternative, enabling faster system access and reducing reliance on traditional credentials. Furthermore, a positive perception of biometric technologies was identified, highlighting ease of use, authentication speed, and improvements in the digital experience.

In conclusion, the implementation of a facial recognition system for accessing institutional platforms can significantly contribute to optimizing authentication processes, providing greater efficiency, security, and usability in the university environment.

Introducción

En las instituciones de educación superior, teniendo como referencia principal la universidad EAN, los sistemas de planificación (ERP) son esenciales para la gestión de procesos académicos y administrativos. SAP es uno de los servicios más utilizados por los estudiantes para realizar procesos esenciales relacionados con notas, matrículas, pagos, certificados y trámites internos.

Sin embargo, a pesar de su importancia, el acceso a este sistema suele presentar dificultades para los estudiantes. Una de las más comunes es la obligatoriedad de cambiar la contraseña periódicamente, lo que genera olvidos constantes, bloqueos de cuenta y pérdida de tiempo en la recuperación. Este problema, aunque no es cotidiano, genera una inconformidad significativa en la experiencia del estudiante.

Con el propósito de mejorar esta problemática en la universidad EAN y la interacción entre los estudiantes y los servicios académicos, este proyecto tiene como objetivo principal el desarrollo y evaluación de un sistema de autenticación biométrica basado en reconocimiento facial, orientado a mejorar el acceso a la plataforma SAP. Para su desarrollo, se utiliza el lenguaje de programación Python junto con librerías especializadas en procesamiento de imágenes, lo que permite implementar un modelo con capacidad de capturar, procesar y comparar información facial para la validación de identidad. También garantiza compatibilidad con computadores, tablets y dispositivos móviles, sin necesidad de que la universidad desarrolle su propio sistema de reconocimiento facial.

En cuanto al alcance, el proyecto se centra en el desarrollo de un prototipo funcional mediante reconocimiento facial, no se tiene contemplada la integración con el sistema de planificación (ERP) SAP en un entorno real, sino que busca analizar la viabilidad técnica de la solución y su nivel de aceptación por los estudiantes de la universidad EAN. Este análisis se construye con la aplicación de una encuesta, lo que permite evaluar la percepción de los estudiantes frente al uso de reconocimiento facial.

Finalmente, el presente documento muestra el proceso de análisis, diseño y desarrollo del prototipo, así como los resultados obtenidos tanto a nivel técnico como desde la perspectiva de los estudiantes de la universidad EAN, con el fin de aportar una base para implementaciones futuras de mecanismos de autenticación biométrica facial en entornos educativos.

Pregunta de investigación

La pregunta que orienta este documento es: ¿Cómo influye la implementación de autenticación biométrica por reconocimiento facial en la experiencia de acceso de los estudiantes de la Universidad EAN en el sistema SAP?

Hipótesis 1: La implementación de un sistema de autenticación biométrica basado en el reconocimiento facial mejora la experiencia de acceso de los estudiantes de la EAN al sistema SAP, en comparación con los modelos tradicionales de autenticación por contraseña, medida a través de indicadores como el tiempo de acceso al sistema, la facilidad percibida de uso y el nivel de satisfacción de los estudiantes.

Hipótesis 2: El uso de modelos de autenticación biométrica basado en reconocimiento facial reduce la frecuencia de bloqueos de cuenta y solicitudes de recuperación de contraseñas asociadas al acceso a SAP, en comparación con el modelo tradicional, evaluado a partir de la frecuencia con que los estudiantes presentan dificultades para acceder al sistema.

Objetivos

Objetivo General:

Diseñar un sistema de autenticación biométrica que permita a los estudiantes acceder a SAP mediante reconocimiento facial, con el fin de mejorar la experiencia de usuario, reducir problemas asociados a la gestión de contraseñas y fortalecer la seguridad del acceso institucional.

Objetivos Específicos:

- Analizar las dificultades que enfrentan los estudiantes en la gestión de contraseñas en el sistema SAP a partir de encuestas aplicadas a estudiantes, identificando la frecuencia de olvidos, bloqueos de cuentas y su impacto en la experiencia de acceso
- Evaluar la viabilidad técnica de las tecnologías de autenticación biométrica basadas en reconocimiento facial mediante la investigación de uso de tecnologías de autenticación biométrica, determinando su viabilidad técnica y compatibilidad con los diferentes dispositivos utilizados por la comunidad estudiantil.
- Desarrollar un prototipo funcional de inicio de sesión biométrica utilizando reconocimiento facial, mediante el lenguaje de programación Python y librerías especializadas como “Face_recognition”, para simular el proceso de inicio de sesión.

- Validar el prototipo desarrollado mediante pruebas de usabilidad con usuarios evaluando indicadores como tiempo de acceso, facilidad de uso, nivel de satisfacción y percepción frente al sistemas.

Definición del problema

En el entorno universitario, el acceso a plataformas institucionales como SAP se basa en mecanismos de autenticación tradicionales con el uso de usuario y contraseñas alfanuméricas. Aunque estas metodologías han perdurado a través de los años por su simplicidad, al momento de aplicarse se presentan limitaciones que afectan la eficiencia del proceso de acceso a los servicios académicos.

Uno de los principales inconvenientes está relacionado con la gestión de credenciales, fundamentalmente debido a las políticas de seguridad que exige la actualización periódica de contraseñas y el uso de combinaciones de mayúsculas, minúsculas, números e incluso símbolos. A pesar de que sea una buena práctica en términos de seguridad, usar este tipo de combinaciones complejas genera dificultades en los estudiantes, como el olvido de claves, errores al ingresar la información y bloqueos temporales de la cuenta, estas situaciones interfieren con el acceso adecuado a la plataforma y puede afectar con el desarrollo normal de los procesos administrativos y académicos.

Además, múltiples estudios señalan que los métodos de autenticación basados en contraseñas presentan vulnerabilidades de seguridad como de usabilidad, lo que ha impulsado la búsqueda de nuevas alternativas más eficientes y centradas en los usuarios (Cataldo et al.,2022). Teniendo esto como referencia la dependencia exclusiva de este tipo

de mecanismos no solo afecta al usuario o estudiante final, sino que también incrementa la generación de mayor cantidad de tickets en la mesa de ayuda generando mayor carga operativa por parte del soporte técnico asociado a la recuperación de accesos. Por tanto, se evidencia la necesidad de implementar nuevas alternativas que permitan optimizar el proceso de autenticación, reduciendo el uso de contraseñas difíciles de retener y mejorando la experiencia de acceso en los sistemas institucionales a los estudiantes de la universidad EAN.

Justificación.

En la actualidad la transformación digital avanza rápidamente causando que la seguridad informática busque soluciones más fuertes para asegurar los datos que son una colección de hechos, números, palabras que mediante análisis se pueden transformar para la toma de decisiones y buscar mejores resultados en un entorno empresarial. En la última década el big data o conjunto de datos grandes y complejos se ha ganado el apodo de “el nuevo petróleo” debido a su valor en el crecimiento empresarial y la innovación (Badman & Kosinski, 2025).

Las nuevas tecnologías implementadas por diversos sectores empresariales usan autenticación sin contraseña o Multifactor de autenticación (MFA), principalmente aquellas basadas en biometría brindan una alternativa segura, eficiente que se adopta a nivel global. El desarrollo del face Id propone un modelo donde el procesamiento biométrico ocurre en el dispositivo del estudiante, sin que se recolecten fotos en el servidor de la universidad, que

podría crear un riesgo crítico de seguridad, proponiendo el uso de los estándares de FIDO Alliance (2021).

En este modelo, el dispositivo del usuario es el encargado de realizar el procesamiento de acceso del machine Learning. Si el rostro coincide el sistema emite una confirmación cifrada hacia SAP. Por tanto, la universidad nunca ve ni almacena los datos biométricos, eliminando la posibilidad de filtraciones de identidad (Shi et al., 2016).

Por consiguiente, desarrollar un sistema de autenticación biométrica para el acceso a SAP mejora no solo una necesidad evidente entre los estudiantes, sino que también representa una oportunidad para modernizar el acceso a plataformas institucionales, reducir los incidentes por bloqueos de cuenta, mejorar la eficiencia operativa y fortalecer la seguridad de datos personales. Asimismo, la implementación de esta solución contribuye a mejorar la experiencia estudiantil, al adoptar nuevas tecnologías y facilitar el uso de servicios académicos, alineándose con las tendencias actuales de innovación.

Marco Teórico

1. Seguridad de la información y control de acceso

La seguridad de la información es entendida como una parte importante de los sistemas digitales que se tienen en la actualidad, destacándose básicamente aquellos por medio de los cuales se gestionan datos y procesos críticos; cuyo objetivo es proteger la información ante cambios o accesos no autorizados e interrupciones que pueden poner en riesgo el normal funcionamiento de una entidad o una empresa. Teniendo en cuenta lo anterior, la seguridad debe tener en cuenta no

solo una infraestructura bien consolidada sino que se contemplen políticas, procesos, procedimientos y componentes que faciliten una gestión adecuada de accesos al sistema.

En este esquema de control el acceso parece ser uno de los elementos más cruciales a tener en cuenta para la seguridad de la información, porque brinda la posibilidad de regular quien tiene autorización para acceder a un sistema y bajo qué condiciones; ese control de acceso es fundamental en los sistemas de autenticación ya que antes de otorgar permisos para acceder a recursos digitales se debe comprobar la identidad de los usuarios, Según Martínez Bresó (2024), la autenticación es un proceso crucial para la gestión de identidades digitales, dado que establece el primer nivel de confianza entre un usuario y un sistema, especialmente en entornos donde la información posee un valor estratégico.

Con el aumento de la digitalización e interconexión de servicios y procesos por parte de las entidades y empresas se han incrementado de igual manera los ataques a los sistemas de información, dejando en evidencia las limitaciones que presentan los modelos actuales para controlar el acceso. Martínez Bresó (2024) señala que los esquemas centralizados de autenticación, ampliamente utilizados en sistemas empresariales y educativos presentan vulnerabilidades estructurales que pueden ser explotadas mediante ataques dirigidos a credenciales de los usuarios o a los servicios que las almacenan. De presentarse dicha situación esta puede ser crítica si se da en una plataforma de una institución educativa ya al presentarse una

falla cuando un usuario se autentique puede afectar o comprometer varios servicios o procesos a la vez.

Por tanto, el artículo consultado destaca la necesidad de fortalecer los mecanismos de control de acceso a través de enfoques más robustos y adaptables que puedan responder al panorama actual de amenazas digitales.

2. Limitaciones de la autenticación basada en contraseñas

Durante años la autenticación basada en contraseñas ha sido el mecanismo más utilizado para controlar el acceso a los sistemas de información. Su rápida y amplia adopción se debe a su facilidad de implementación y bajo costo operativo. Sin embargo, el crecimiento de los entornos digitales y el creciente ataque informático han evidenciado múltiples debilidades en este modelo de autenticación tradicional.

Viéndolo desde una perspectiva técnica, las contraseñas presentan vulnerabilidades inherentes relacionadas con el uso y gestión por parte de los usuarios. (Martinez - 2023) explica que muchos de los sistemas dependen de esquemas centralizados de almacenamiento de credenciales, lo que los convierte en objetivos atractivos para ataques como phishing, fuerza bruta o robo de bases de datos. A demás también menciona que el uso repetido de la misma contraseña y la tendencia de los usuarios a usar combinaciones débiles incrementan significativamente el riesgo de accesos no autorizados.

Siguiendo este mismo hilo de investigación académica desarrollada en el ámbito universitario se ha demostrado que el factor humano constituye uno de los

principales puntos débiles de la autenticación basada en contraseñas. Un estudio de la universidad de los Andes destaca que los usuarios suelen preferir y priorizar la memorización sobre la seguridad, lo que conduce al uso de contraseñas simples o reutilizadas en múltiples plataformas, reduciendo así la efectividad de este mecanismo como barrera de protección (Heim Jaramillo, n.d.)

Asimismo, la dependencia exclusiva de contraseñas dificulta detectar si la persona que entra con esas credenciales es realmente el usuario legítimo. (Martínez - 2023) una vez comprometida la contraseña, el sistema pierde la capacidad de diferenciar un acceso autorizado y uno malicioso, lo que evidencia la necesidad de importar factores adicionales de autenticación que refuercen el control del acceso.

Como resultado, de estas investigaciones se coincide en que la autenticación basada solo en contraseñas resulta inadecuada para enfrentar los desafíos actuales de seguridad de la información. Estas limitaciones han impulsado la evolución a nuevos modelos de autenticación más sólidos como la autenticación multifactorial y los modelos biométricos, que buscan disminuir la dependencia de las mismas credenciales y reducir los riesgos asociados al factor humano.

3. Autenticación Multifactor (MFA)

Ante las limitaciones que presenta la autenticación basada únicamente en contraseñas, al pasar del tiempo han surgido mecanismos más robustos que buscan fortalecer los procesos de verificación de identidad en los sistemas informáticos. Uno de los enfoques más utilizados actualmente es la autenticación Multifactor (MFA), la cual combina diferentes tipos de credenciales para validar que un usuario

es realmente quien dice ser.

Según Morales, Fierrez y colaboradores (2015), los sistemas de autenticación modernos se fundamentan en la combinación de múltiples factores que pueden clasificarse generalmente en tres categorías: algo que el usuario sabe (como una contraseña o PIN), algo que el usuario posee (como un token, un dispositivo móvil o una tarjeta inteligente) y por último algo que el usuario es, como las características biométricas como la huella dactilar o el reconocimiento facial. La integración de estos mecanismos posibilita una disminución del riesgo de accesos no autorizados, ya que un atacante tendrá que comprometer más de un mecanismo de seguridad para conseguir ingresar al sistema.

En el panorama de las infraestructuras actuales, la autenticación Multifactor es un elemento fundamental en las estrategias de ciberseguridad. En la actualidad varias entidades y empresas están implementado el sistema de Autenticación Multifactor (MFA) de la mano de mecanismos de inicio de sesión único (SSO), sin la necesidad del uso de contraseñas con el fin de mejorar y proteger la experiencia y seguridad del usuario. Se enfatiza, en particular, que estos sistemas permiten aplicar controles cuando se detectan comportamientos inusuales durante el inicio de sesión, como accesos desde dispositivos desconocidos o intentos de conexión fuera de los horarios habituales (SecureBridge,2025).

Los sistemas de MFA de última generación, además de su implementación meticulosa funcionan con políticas basadas en el riesgo. Esto permite un equilibrio entre seguridad y facilidad de uso: el sistema "aprende" el contexto del usuario y

solo solicita factores adicionales cuando las condiciones sugieren una amenaza potencial (SecurityBridge, 2025). Así se protege al usuario en entornos de confiables, y al mismo tiempo se fortalece la barrera ante cualquier patrón sospechoso.

4. Autenticación Biométrica

Actualmente los sistemas de autenticación han incorporado mecanismos biométricos como una opción más segura que los métodos convencionales, que solo se basan en las contraseñas. La autenticación biométrica se basa en la utilización de rasgos físicos o comportamientos únicos de las personas, como lo son la huella dactilar, el reconocimiento facial, el iris o incluso patrones de comportamiento. Estas cualidades hacen que la comprobación de la identidad de un usuario sea más fiable, dado que son difíciles de imitar o trasladar entre personas.

Según Jain, Ross y Prabhakar (2004) un sistema biométrico está compuesto generalmente por cuatro componentes principales: el módulo de adquisición de datos biométricos, el sistema de extracción de características, el mecanismo de comparación con plantillas almacenadas y el módulo de decisión que determina si existe una coincidencia válida. Este proceso permite identificar o autenticar a un usuario mediante el análisis de patrones biométricos previamente registrados en el sistema.

También es necesario evaluar el rendimiento de los sistemas biométricos a través de indicadores que hagan posible la medición de su exactitud. La tasa de

rechazo falso (FRR) y la tasa de aceptación falsa (FAR) son dos métricas muy empleadas. La primera refleja la posibilidad de que un usuario legítimo sea rechazado en el proceso de autenticación; la segunda, por su parte, mide la probabilidad de que el sistema acepte a un usuario no autorizado. Estas medidas posibilitan examinar el balance entre la seguridad y la facilidad de uso en un sistema biométrico, pues si es muy restrictivo puede causar problemas a los usuarios legítimos, y si es muy flexible podría poner en riesgo la seguridad del sistema (Daugman, 2003).

5. Reconocimiento Facial como Método Biométrico

El reconocimiento facial se ha consolidado como una de las tecnologías modernas más adoptadas en los sistemas de autenticación. A diferencia de otros métodos, esta técnica aprovecha algoritmos de visión por computador y modelos de aprendizaje profundo (Deep Learning) para identificar o verificar a una persona a partir de características únicas de su rostro. Los sistemas actuales utilizan redes neuronales profundas capaces de extraer representaciones discriminativas del rostro humano, lo que permite comparar imágenes con bases de datos previamente registradas con altos niveles de precisión (Wang et al., 2021).

Un avance significativo en esta área ha sido la implementación de FaceNet, que posibilitan convertir imágenes faciales en representaciones matemáticas dentro de un espacio vectorial. Este enfoque facilita la comparación entre rostros mediante el cálculo de distancias entre vectores, lo que mejora notablemente la precisión en procesos de identificación y verificación de identidad (Schroff et al., 2015)

6. Paradigmas de Procesamiento: Edge AI y Privacidad desde el Diseño

Dentro de la investigación de arquitecturas biométricas, se encuentra indispensable definir donde debe ocurrir el procesamiento del rostro.

Tradicionalmente, los sistemas dependían de un servidor local (nube) al que se le enviaban los datos sensibles por la red para hacer el análisis, Sin embargo, para este prototipo se planea usar el uso de Edge IA (inteligencia Artificial en el borde), donde el modelo de reconocimiento se ejecuta en el dispositivo del estudiante.

Este enfoque desarrollo se fundamenta en los principios de privacy by design (Privacidad desde el diseño). Según Cavoukian (2011), la seguridad debe ser una característica propia del sistema. Al procesar la biometría “on.device”, el patron facial nunca abandona el dispositivo móvil. El sistema solo comunica a la plataforma SAP un código de confirmación cifrado, asegurando que la universidad EAN no asuma el resguardo de los datos biométricos y reduciendo la superficie de ataque de los ciberdelincuentes.

Por último, al adoptar estos avances de autenticación permite implementar modelos de autenticación más seguros. Como indican Whitman y Mattord (2021), el reconocimiento facial desplaza la carga de la seguridad desde la memoria del usuario hacia sus características físicas irrepetibles, fortaleciendo la confianza de acceso a sistemas críticos institucionales y mitigando los riesgos asociados a suplantación de identidad.

7. Aplicación de tecnologías de autenticación en entornos universitarios

El crecimiento de las plataformas digitales en las instituciones educativas ha incrementado la necesidad de implementar mecanismos de seguridad que permitan proteger la información académica y garantizar la autenticidad de los usuarios que acceden a los sistemas institucionales. El uso de entornos virtuales de aprendizaje, sistemas de gestión académica y plataformas de evaluación en línea ha generado nuevos desafíos relacionados con la verificación de identidad de los estudiantes.

Diversos estudios han señalado que los sistemas tradicionales de autenticación basados únicamente en contraseñas presentan limitaciones importantes en términos de seguridad, debido a su vulnerabilidad frente a ataques como el phishing, el robo de credenciales o la reutilización de contraseñas en múltiples servicios (Ometov et al., 2020). Como consecuencia, muchas instituciones han comenzado a implementar mecanismos de autenticación Multifactor que permiten fortalecer los procesos de control de acceso.

La autenticación Multifactor combina diferentes tipos de evidencia para verificar la identidad de un usuario, como algo que el usuario conoce (contraseña), algo que posee (dispositivo móvil o token) o algo que es (biometría). Este enfoque permite reducir significativamente el riesgo de accesos no autorizados a los sistemas institucionales y mejorar la protección de los recursos digitales (Whitman & Mattord, 2021).

En el contexto de las instituciones universitarias, la implementación de tecnologías de autenticación avanzada puede contribuir a mejorar la seguridad de las plataformas educativas y a garantizar la integridad de los procesos académicos. Por esta razón, el presente proyecto analiza la implementación de mecanismos de autenticación multifactor como una estrategia para fortalecer la seguridad en el acceso a sistemas institucionales y reducir los riesgos asociados a la suplantación de identidad en entornos digitales.

8. Sistemas empresariales SAP y seguridad en la autenticación

Los sistemas SAP (Systems, Applications and Products in Data Processing) constituyen una de las plataformas de planificación de recursos empresariales (ERP) más utilizadas a nivel mundial para la gestión de procesos organizacionales. Estas plataformas permiten integrar múltiples funciones empresariales, como finanzas, logística, recursos humanos y gestión de operaciones, dentro de un mismo entorno tecnológico. Sistemas modernos como SAP S/4HANA han sido diseñados para procesar grandes volúmenes de información empresarial y soportar procesos críticos de negocio mediante arquitecturas basadas en bases de datos en memoria y entornos cloud (SAP SE, 2021).

Debido a la importancia de la información que gestionan estos sistemas, la seguridad y el control de acceso representan aspectos fundamentales en la administración de entornos SAP. Las plataformas SAP incorporan diversos mecanismos de autenticación que permiten verificar la identidad de los usuarios antes de acceder a los recursos del sistema. Entre estos mecanismos se encuentran la

autenticación mediante usuario y contraseña, certificados digitales, autenticación mediante tickets de sesión y tecnologías de inicio de sesión único (Single Sign-On), que permiten a los usuarios acceder a múltiples aplicaciones empresariales utilizando una sola autenticación inicial.

Dentro de estas alternativas, las tecnologías biométricas han ganado relevancia debido a su capacidad para verificar la identidad de los usuarios a partir de características físicas o comportamentales únicas. El reconocimiento facial, en particular, se ha convertido en una de las soluciones biométricas más utilizadas en sistemas de autenticación modernos, gracias a los avances en algoritmos de visión por computador y aprendizaje profundo que permiten identificar rostros con altos niveles de precisión (Wang et al., 2021). Estas tecnologías pueden integrarse con plataformas empresariales para ofrecer mecanismos de autenticación más seguros y eficientes.

En el contexto de este proyecto, la implementación de un sistema de autenticación basado en reconocimiento facial (Face ID) para el acceso a SAP busca mejorar la seguridad y la experiencia de usuario en el proceso de inicio de sesión. Al sustituir o complementar las contraseñas tradicionales con mecanismos biométricos, es posible reducir los riesgos asociados al robo de credenciales y facilitar un acceso más rápido y confiable a los sistemas institucionales. De esta manera, el uso de tecnologías biométricas en entornos empresariales representa una alternativa

prometedora para fortalecer la protección de la información y optimizar los procesos de autenticación en plataformas críticas.

Estado del arte (Metodología Prisma)

En la siguiente sección se desarrolló mediante una investigación, revisión y análisis de diferentes fuentes de información como bases de datos, se desarrolló siguiendo la metodología prisma, con el propósito de identificar, seleccionar y analizar estudios científicos recientes, relacionados con la autenticación biométrica, el reconocimiento facial y la seguridad en el acceso a sistemas de información institucionales.

Proceso de Búsqueda y selección

La búsqueda se centró en artículos y revista indexadas en Google Académico y bases de datos como Proquest, Web of Science y Scopus usando diferentes ecuaciones de búsqueda con operadores booleanos:

(face recognition OR facial authentication)(biometric authentication OR multi factor authentication)

("education systems" OR "information systems security")

Se estableció un periodo temporal de 2020-2026, con el fin de garantizar el uso de referencias actuales, se incluyeron publicaciones en idiomas inglés y español. Los tipos de documentos seleccionados fueron artículos de investigación original y revisiones sistemáticas.

Criterios de Inclusión y Exclusión

Inclusión (CI): Artículos publicados en revistas indexadas en Google académico y las bases de datos son Proquest, Web of Science y Scopus entre 2020 y 2026, que abordan temas como autenticación Multifactor, publicaciones con plataformas educativas o artículos que analicen la seguridad de datos biométricos.

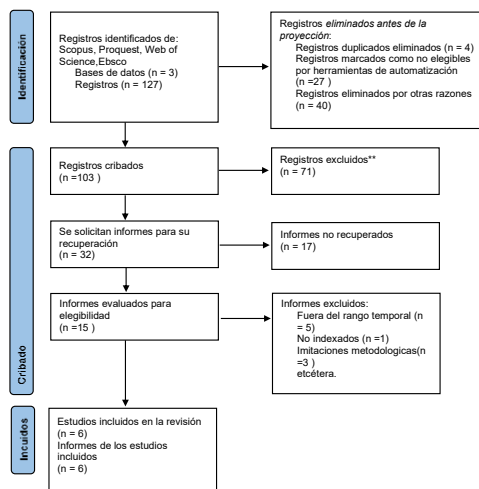
Exclusión (CE): Artículos de opinión, artículos duplicados, estudios no relacionados con sistemas digitales y publicaciones anteriores al año 2020

Diagrama de Flujo

Tabla 1

Metodología Prisma

Identificación de estudios via bases de datos y archivos



*Consider, if feasible to do so, reporting the number of records identified from each database or register searched (rather than the total number across all databases/registers).

**If automation tools were used, indicate how many records were excluded by a human and how many were excluded by automation tools.

Fuente: Elaboración propia

Análisis crítico y comparativo

Después de la revisión sistémica, se revela una transición significativa en la biometría facial: de sistemas basados en la nube a modelos descentralizados, A continuación, se muestra una tabla comparativa que permite la visualización simplificada de los hallazgos de los estudios seleccionados.

Tabla 2

Comparación de estudios mediante la revisión Prisma

Autor(es) / Año	Título del estudio	Objetivo principal	Metodología empleada	Variables analizadas	Principales hallazgos	Limitaciones reportadas	Relación con el proyecto actual
Wang et al. (2021)	Deep learning for face recognition: A survey	Analizar los avances del reconocimiento facial basado en deep learning.	Revisión sistemática de algoritmos CNN y modelos de reconocimiento facial.	Precisión, robustez, algoritmos de reconocimiento.	Los modelos de deep learning mejoran significativamente alcanzando más del 99% de precisión de los sistemas biométricos.	Dependencia de grandes volúmenes de datos de entrenamiento. Además, el modelo presenta sensibilidad a cambios de iluminación extremos	Proporciona bases teóricas para implementar sistemas de autenticación facial.
Ometov et al. (2020)	Multi-factor authentication: A survey	Analizar los métodos actuales de autenticación multifactor.	Análisis comparativo de protocolos de autenticación multifactor: contraseñas, tokens, biometría y comportamiento	Seguridad, usabilidad, factores de autenticación.	MFA aumenta significativamente la seguridad en sistemas digitales. La biometría es el factor con mayor usabilidad por parte de los usuarios	Complejidad en la implementación en sistemas empresariales.	Justifica el uso de biometría como factor adicional de autenticación complementario o sustituto del modelo de acceso con contraseña en SAP
Hossain & Muhammad (2020)	Cloud-assisted secure biometric authentication	Proponer un sistema biométrico seguro basado en	Diseño experimental y evaluación del sistema.	Precisión, seguridad, eficiencia del sistema.	Los sistemas biométricos pueden mejorar el control de acceso en plataformas digitales.	Dependencia de infraestructura tecnológica adecuada.	Apoya el desarrollo de sistemas biométricos para autenticación,

		reconocimiento facial.					sin que la universidad requiera su propio servidor de reconocimiento facial
Shen et al. (2022)	Face recognition-based authentication system using deep learning	Desarrollar un sistema de autenticación facial basado en redes neuronales.	Implementación experimental con modelos de deep learning.	Tasa de reconocimiento, seguridad del sistema.	Se lograron altos niveles de precisión en la verificación de identidad.	Sensibilidad a condiciones de iluminación y calidad de imagen.	Relacionado con el desarrollo de sistemas Face ID para acceso a plataformas digitales.
Garcia-Pavon (2022)	Reconocimiento facial y protección de datos: Una perspectiva legal	Analizar el impacto del reconocimiento facial en la privacidad y el tratamiento de datos personales	Revisión normativa y jurisprudencial sobre la protección de datos	Consentimiento informado, habeas data, almacenamiento biométrico y ética	La biometría facial es un dato sensible que requiere de medidas de seguridad técnicas reforzadas y no solo legales	La legislación suele avanzar más lento que la innovación digital, creando vacíos legales.	Sustenta la necesidad de no guardar datos en el servidor de la universidad EAN para cumplir con leyes de protección de datos.
Rukhiran et al. (2023)	IoT Based Biometric Recognition Systems in Education for Identity Verification	Evalúa la calidad y efectividad de sistemas biométricos IoT para la verificación de identidad estudiantil	Estudio comparativo experimental con múltiples modalidades biométricas (facial, iris, huella, en entorno universitario)	Precisión biométrica, tiempo de verificación, aceptación del usuario escalabilidad del sistema	El reconocimiento facial obtuvo la mayor aceptación por parte de los estudiantes. Los sistemas IoT biométricos reducen en un 78% el tiempo de verificación frente al método manual.	Requiere dispositivos con cámara de resolución mínima. Retos de privacidad asociados al almacenamiento de datos biométricos	Es uno de los antecedentes más directos, ya que aborda biometría en la educación superior con estudiantes como usuarios finales, contexto equivalente al de la universidad EAN.

Síntesis de hallazgos y Brechas Identificadas

Los artículos seleccionados comparten un interés en mejorar el acceso a plataformas mediante la autenticación digital por biometría, sin embargo, tienen perspectivas diferentes en metodología y alcance. Wang et al. (2021) y Shen et al. (2022) se centran en el desarrollo técnico con modelos de aprendizaje profundo, mientras que otros autores como Ometov et al. (2020) y Hoissain & Muhammad (2020) se basan en un análisis hacia sistemas Multifactor y arquitecturas distribuidas en la nube. Rukhiran et al. (2023) aborda directamente al contexto de educación superior, comparando tecnologías biométricas para la verificación de identidad estudiantil mediante IoT que lo convierte en un antecedente más para el desarrollo del presente proyecto.

Predomina una metodología en enfoques experimentales con modelos basados en Deep Learning (CNN, FaceNet) para el reconocimiento facial, esta metodología se combina con tecnologías de autenticación Multifactor. Algo que comparten en común es que no solo evalúan la viabilidad técnica, sino que también buscan priorizar la experiencia de usuario y los retos en la protección de datos. Algunos vacíos predominantes identificados: no se encontró evidencia de algún estudio que abordara específicamente la integración del reconocimiento facial con sistemas ERP como SAP en entornos educativos universitarios, tampoco evalúan directamente la percepción de los estudiantes frente al cambio del modelos de contraseñas alfanuméricos hacia la biometría en este tipo de plataformas, y por último existe ausencia de prototipos funcionales desarrollados con herramientas de código

abierto como Python y la librería face_recognition, orientadas a la implementación en instituciones de educación superior con recursos tecnológicos limitado

Los vacíos identificados, justifican la oportunidad del presente trabajo en desarrollar un reconocimiento facial para acceder al sistema de centralización de servicios SAP mejorar la experiencia de los estudiantes

Metodología

La presente investigación se desarrolla bajo un enfoque mixto que integra, por un lado, la recolección y análisis de datos cuantitativos orientado a caracterizar la experiencia de los estudiantes con el sistema SAP y su percepción frente a implementar tecnologías biométricas, por otro lado, un componente tecnológico cualitativo orientado al diseño y construcción de un prototipo funcional de autenticación mediante reconocimiento facial. La combinación de esta metodología permite correlacionar los objetivos centrales de la investigación; permite comprender la problemática desde la experiencia de los estudiantes de la EAN y demostrar técnicamente la viabilidad de la solución propuesta.

Enfoque y alcance de la investigación

El diseño es no experimental transversal, ya que la recolección de datos se realiza en un único momento temporal sin manipulación de variables, sino que por el contrario se describieron y analizaron las condiciones actuales de acceso al sistema SAP y se evaluó también la disposición a usar biometría facial. La recolección de datos se realizó en el mes de febrero de 2026, garantizando el uso de perspectivas actuales.

El alcance de la investigación es descriptivo-propositivo, porque busca caracterizar las perspectivas y comportamiento de los estudiantes frente a los mecanismos de autenticación actuales, y aplicado porque se deriva en el desarrollo de un prototipo funcional evaluable.

Diversas investigaciones han señalado que los sistemas biométricos pueden mejorar significativamente los niveles de seguridad en plataformas digitales, especialmente cuando se apoyan en modelos de aprendizaje profundo para el reconocimiento facial (Wang et al., 2021; Shen et al., 2022).

Población y Muestra

La población de estudio estuvo conformada por estudiantes activos de la universidad EAN que utilizan el sistema SAP, el muestreo fue no probabilístico por conveniencia, en el que la participación fue voluntaria y se canalizó a partir de grupos académicos de la universidad y de compañeros de clase.

Se recibieron 97 respuestas en total, después de aplicar un criterio de inclusión principal, el cual era ser estudiante activo de la universidad, la muestra definitiva quedó conformada por 87 participantes, los registros restantes corresponden a personas que no estaban activas en la universidad y fueron excluidos del análisis. La siguiente tabla resume las características sociodemográficas de la muestra.

Tabla 3

Perfil sociodemográfico (n=87)

Variable	Categoría	n (%)
Semestre	7.º – 8.º	51 (58,6 %)
	5.º – 6.º	18 (20,7 %)
	1.º – 2.º	11 (12,6 %)
	3.º – 4.º	7 (8,0 %)
Programa	Ingeniería de Sistemas	~28 (32,2 %)
	Lenguas Modernas	~23 (26,4 %)
	Otros programas	36 (41,4 %)
Total muestra válida	—	87 (100 %)

Fuente: Elaboración Propia

Instrumentos de recolección de Información: Encuesta estructurada

Se diseñó una encuesta estructurada, diseñada en Microsoft Forms y distribuida por medio de la red social de WhatsApp a los grupos de materias académicas de la EAN durante el mes de febrero de 2026. El formulario constó de 15 preguntas, 15 cerradas y una abierta, organizadas en tres (3) secciones temáticas.

- Sección 1 (Perfil del encuestado): consta de 3 preguntas, las cuales recogen información sobre programa académico, semestre y si el estudiante es activo o no, hace el filtro para caracterizar la muestra válida.
- Sección 2 (Uso y experiencia con SAP): Consta de 16 preguntas que exploran la frecuencia y uso de SAP, la incidencia de olvidos, bloqueos de cuenta, la experiencia en el uso y el impacto en el cambio periódico de contraseña.

- Sección 3 (Autenticación Biométrica): Consta de 3 preguntas que indaga sobre el uso previo de autenticación en dispositivos personales y si tiene o no preocupación entorno a la privacidad de datos biométricos.

La escala de medición varió dependiendo de la pregunta, preguntas de (SI/NO) para variables de incidencia, escala Likert y escalas numéricas de 1 a 10 para variabilidad de percepción y preguntas de selección múltiple, la siguiente tabla muestra el orden de las preguntas.

Tabla 4

Diseño de la encuesta aplicada a estudiantes de la EAN

Nº	Pregunta	Variable medida	Tipo de respuesta
1	¿Eres estudiante activo de la Universidad EAN?	Criterio de elegibilidad	Sí / No
2	¿Qué programa académico cursas actualmente?	Perfil demográfico	Abierta
3	¿Qué semestre estás cursando?	Perfil demográfico	Opciones: 1-2, 3-4, 5-6, 7-8+
4	¿Con qué frecuencia utilizas el sistema SAP?	Intensidad de uso de SAP	Escala nominal (4 opciones)
5	¿Has olvidado tu contraseña de SAP alguna vez?	Frecuencia de olvido de credenciales	Escala nominal (4 opciones)
6	¿Has tenido bloqueos de cuenta en SAP?	Incidencia de bloqueos	Sí / No
7	¿Cómo calificarías tu experiencia actual para iniciar sesión en SAP?	Satisfacción con el método actual	Escala Likert 1-5
8	¿El cambio periódico de contraseña afecta tu experiencia como estudiante?	Impacto percibido de la política de contraseñas	Escala nominal (4 opciones)

9	¿Utilizas biometría en tus dispositivos personales?	Familiaridad previa con biometría	Sí / No / Otro
10	¿Qué tan familiarizado(a) estás con la autenticación biométrica?	Nivel de conocimiento biométrico	Escala Likert 5 niveles
11	¿Te sentirías cómodo(a) usando Face ID para acceder a SAP?	Aceptación de la solución propuesta	Sí / No / No estoy seguro
12	¿Qué beneficios ves en la biometría para SAP?	Percepción de beneficios	Selección múltiple ordenada
13	¿Crees que eliminar contraseñas mejoraría tu experiencia?	Disposición al cambio	Sí / Tal vez / No
14	¿Qué tan viable ves implementar biometría en la universidad?	Viabilidad percibida	Escala 0-10
15	¿Te preocuparía el uso de datos biométricos?	Preocupación por privacidad	Sí / No / Tal vez

Fuente: elaboración propia.

Componente Tecnológico: Prototipo de Reconocimiento Facial

El prototipo funcional de autenticación biométrica utilizando el lenguaje de programación Python, el propósito del prototipo no es integrarse en producción con el sistema SAP lo que excede el alcance del proyecto, si no demostrar la viabilidad técnica de la solución planteada y permitir una evaluación de su funcionamiento en profesores o estudiantes.

El prototipo se desarrolla en una arquitectura de redes neuronales profundas para la verificación de identidad, el procedimiento técnico sigue tres etapas claves en el código implementado:

1. **Detección y Normalización:** Se emplea la librería MTCNN para la localización de rostros. Este método permite redimensionar la entrada a 160x160 píxeles y aplicar un post-procesamiento de alineación, garantizando que el modelo reciba datos estandarizados (Shen et al., 2022).
2. **Extracción de Embeddings:** Se utiliza el modelo InceptionResnetV1 pre entrenado. Este componente traduce las facciones en un vector numérico (embedding), lo que permite realizar comparaciones matemáticas sin necesidad de almacenar imágenes faciales reales, alineándose con el principio de Privacy by Design (García-Pabón, 2022).
3. **Clasificación y Verificación:** Se implementó un algoritmo SVC (Support Vector Classification) con núcleo lineal. Esta técnica permite clasificar los vectores generados en tiempo real frente a los patrones registrados, determinando el acceso mediante una estimación de probabilidad de coincidencia.

La siguiente tabla muestra los componentes, librerías y modelos utilizados en el desarrollo del código de Python argumentando la función y justificación de su implementación en el reconocimiento facial

Tabla 5

Componentes Desarrollo del código

Componente / Librería	Versión / Modelo	Función en el Desarrollo	Justificación Técnica
Lenguaje de Programación	Python 3.x	Lenguaje base para la implementación del algoritmo.	Alta compatibilidad con librerías de visión artificial y <i>Deep Learning</i> .
Detección Facial	MTCNN (<i>Multi-task Cascaded Convolutional Networks</i>)	Localización, alineación y redimensionamiento de rostros a 160x160 px.	Permite preparar el rostro para la extracción de características, ignorando el fondo.

Extracción de Embeddings	InceptionResnetV1 (Preentrenado en <i>VGGFace2</i>)	Generación del vector matemático (128-512 dimensiones) que representa el rostro.	Traduce rasgos físicos en datos numéricos, cumpliendo con la "Privacidad desde el Diseño".
Visión Artificial	OpenCV (<i>Open Source Computer Vision Library</i>)	Captura de video en tiempo real, dibujo de cuadros delimitadores y manejo de frames.	Estándar de la industria para procesamiento de video con baja latencia.
Clasificación de Identidad	SVC (<i>Support Vector Classification</i>) de Scikit-Learn	Comparación de los vectores en tiempo real para determinar la identidad del usuario.	Alta precisión en clasificación con muestras de datos pequeñas (pocos usuarios registrados).
Procesamiento Numérico	NumPy	Manipulación de arreglos multidimensionales y operaciones matemáticas vectoriales.	Optimiza el rendimiento del sistema al manejar los <i>embeddings</i> como tensores.
Pre-procesamiento	Normalizer (L2)	Normalización de los vectores antes de la clasificación.	Asegura que las variaciones de escala en los datos no afecten la precisión de la comparación.
Persistencia de Datos	Pickle	Almacenamiento y carga del modelo de clasificación entrenado.	Permite que el sistema reconozca a los usuarios registrados sin re-entrenar cada vez que se inicia.

Fuente: elaboración propia.

Los sistemas biométricos han demostrado ser herramientas eficaces para fortalecer los mecanismos de autenticación digital, ya que permiten identificar características físicas únicas de los usuarios, reduciendo el riesgo de suplantación de identidad (Hossain & Muhammad, 2020).

Técnicas para el análisis de la información

A partir de los datos recolectados por la encuesta se realiza un análisis mediante estadística descriptiva, usando porcentajes y frecuencias para identificar patrones en las respuestas de los estudiantes. El resultado del análisis permitirá determinar el nivel de aceptación de los usuarios frente a la implementación de autenticación biométrica en sistemas institucionales.

Por otra parte, el desarrollo del prototipo de reconocimiento facial permitirá evaluar de manera conceptual la viabilidad técnica de implementar este tipo de tecnología en sistemas de acceso como SAP. La combinación del análisis de percepción de los usuarios y el desarrollo del prototipo permitirá formular una propuesta orientada a mejorar la seguridad y la experiencia de autenticación en plataformas institucionales.

Resultados y Análisis

Esta sección muestra los hallazgos obtenidos a partir de los componentes de investigación, en la parte de análisis cuantitativo de la encuesta aplicada a estudiantes activos de la universidad EAN (n=87) y por otro lado en los resultados funcionales del prototipo de autenticación biométrica

Resultado encuesta (Componente cuantitativo)

La encuesta fue respondida por 97 personas, de las cuales 87 cumplieron el requerimiento de ser estudiantes activos de la universidad EAN. La investigación muestra una concentración en semestres avanzados: el 58,6 % cursaba séptimo u octavo semestre, seguido por el 20,7 % en quinto o sexto. Esta distribución es relevante porque implica que la mayoría de los participantes encuestados tiene mayor trayectoria de uso del sistema SAP al estar vinculado a la universidad por varios años y, por tanto, mayor experiencia con los problemas de autenticación.

Sección 1 Experiencia de uso SAP y gestión de contraseñas

El 54 % de los estudiantes usa SAP de forma ocasional y el 31,0 % varias veces por semana, lo que indica que los estudiantes la usan habitualmente. Estos datos muestran la importancia del proceso de autenticación, ya que no se trata de un uso irregular, sino de una interacción recurrente que depende de su funcionamiento puede impactar positiva o negativamente experiencia del estudiante.

Figura 1

Frecuencia uso de SAP

4. ¿Con qué frecuencia utilizas el sistema SAP?



Por otro lado, respecto a la gestión de las contraseñas se evidenció que el 86% de los estudiantes ha olvidado la contraseña de SAP por lo menos una vez, solo el 13.8% seleccionó que no ha tenido inconvenientes en el acceso, se puede inferir que los estudiantes olvidan sus credenciales de acceso siendo un problema recurrente entre los estudiantes de la universidad EAN

Tabla 6

Frecuencia olvido de contraseña en SAP

Categoría de respuesta	n	%
Varias veces	39	44,8 %
1 o 2 veces	20	23,0 %
Con mucha frecuencia	16	18,4 %
Nunca	12	13,8 %

Teniendo en cuenta el análisis de la sección uno, el 58,6% de los estudiantes encuestados informa que ha sufrido de bloqueos en la cuenta SAP por problemas por la contraseña, a partir de esos datos podemos evidenciar que al momento de bloqueo de cuenta se interrumpe el acceso al sistema, generando consecuencias sobre inscripción de materias, consulta de notas, consulta de horario etc.

Por otro lado el al evaluar la experiencia en el inicio de sesión con SAP mediante la escala de Likert de 1 a 5, muestra que el 74,7% de los estudiantes tiene una experiencia de 3 o 4, siendo la media 3,48 y la mediana de 4,0, lo que indica que la percepción de los estudiantes con la plataforma es positiva pero con posible mejora, ya que solo el 11,5% selecciono una calificación de 5, mientras que el 13,8% calificó con 1 o 2, presentando inconformidad con su acceso.

Figura 2

Calificación de la experiencia de inicio de sesión en SAP escala likert 1-5(n=87) Media= 3.48

7. ¿Cómo calificarías tu experiencia actual para iniciar sesión en SAP?

[Más detalles](#)



Elaboración Propia

Sobre el impacto que genera el cambio periódico de contraseña, el 82,8 % de los estudiantes indicó que esta política afecta de alguna forma su experiencia: el 28,7 % de manera significativa y el 54,0 % de forma leve. Únicamente el 13,8 % menciona que no le afecta. El análisis de estos resultados está relacionado con las investigaciones de los artículos revisados, que señalan que las políticas de renovación periódica de contraseñas incrementan los errores de gestión de credenciales sin mejorar proporcionalmente la seguridad (Ometov et al., 2020).

Figura 3

Percepción del impacto de cambio de contraseña periódico

8. ¿Consideras que el proceso de cambio periódico de contraseña afecta tu experiencia como estudiante?



Sección 2 Uso y experiencia al usar SAP

Esta sección se centró en analizar como los estudiantes perciben y aceptan la autenticación biométrica, el primer hallazgo es que el 93,3% de los estudiantes usa actualmente algún método de autenticación biométrica en sus dispositivos personales cómo podría ser (reconocimiento facial o huella dactilar), con estos datos se puede evaluar la viabilidad de la solución propuesta, ya que la mayoría de los encuestados tienen familiaridad con esta tecnología eliminando así la problemática de implementación de sistemas biométricos, por la resistencia al cambio por desconocimiento.

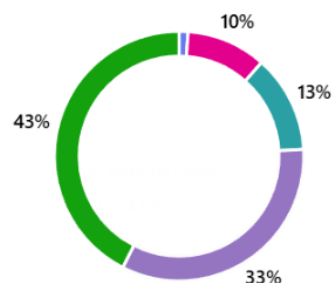
En la siguiente ilustración el 75.8% de los encuestados está familiarizado o muy familiarizado con el uso de la autenticación biométrica, mientras que solo el 11,4% tiene niveles bajos de familiaridad.

Figura 4

Nivel de familiaridad con autenticación Biométrica

10. ¿Qué tan familiarizado(a) estás con el uso de autenticación biométrica?

● Nada familiarizado	1
● Poco familiarizado	9
● Medianamente familiarizado	11
● Familiarizado	29
● Muy familiarizado	37



Frente a la propuesta de implementar Face ID para acceder a SAP, el 89,7% de los estudiantes están interesados y les llama la atención, por el contrario, el 6,9% de los estudiantes tienen inseguridad en usarlo, y solo el 3,4% indicó no estar dispuesto a usarlo, Con estos resultados se confirma que la mayoría de estudiantes tienen disposición a implementar el proyecto.

Figura 5

Adopción de Implementación de autenticación Biométrica

11. ¿Te sentirías cómodo(a) utilizando Face ID u otro método biométrico para acceder al sistema SAP?



En la pregunta de selección múltiple sobre los beneficios observados de implementar biometría en SAP, en la siguiente tabla e ilustración se muestra la jerarquía de los resultados, indicando que los estudiantes priorizan la eficiencia y la simplicidad del proceso sobre la seguridad.

Tabla 7

Beneficios percibidos de implementar biometría en SAP — selección múltiple (n = 87)

Categoría de respuesta	n	%
Acceso más rápido	62	71,3 %
Reducción del uso de contraseñas	39	44,8 %
Menos bloqueos de cuenta	17	19,5 %
Mayor comodidad	16	18,4 %

Mayor seguridad	13	14,9 %
No considera que tenga beneficios	1	1,1 %

Figura 6

Beneficios de implementación de Biometría en SAP

12. ¿Qué beneficios consideras que tendría implementar autenticación biométrica en SAP? (Organiza de forma descendente)



El 83 % de los estudiantes consideró que un sistema de acceso sin contraseñas mejoraría su experiencia como estudiante, el 16 % respondió tal vez y solo 1 participante 1% consideró que no mejoraría. En términos de viabilidad percibida, evaluada en escala de 0 a 10, la media fue de 8,46 y la mediana de 9,0. El 58,6 % otorgó una puntuación de 9 o 10, mostrando que los estudiantes tienen una percepción favorable sobre la posibilidad de implementar el Face ID en la universidad.

Tabla 6

Viabilidad percibida de implementación de biometría en la universidad, escala de 1-10

Categoría de respuesta	n	%
------------------------	---	---

Puntuación 10	28	32,2 %
Puntuación 9	23	26,4 %
Puntuación 8	13	14,9 %
Puntuación 7	14	16,1 %
Puntuación 6	7	8,0 %
Puntuación 5 o menor	2	2,3 %

Por último, con respecto a la preocupación por el uso al usar datos biométricos, el 55% de los estudiantes indico que no le preocuparía, el 37% respondió que tal vez y solo el 8% manifestó tener preocupación. Estos resultados, sugieren que algunos estudiantes en su minoría tienen preocupación por sus datos y la mayoría no percibe preocupación significativa en adoptar este tipo de sistemas.

Figura 7

Preocupación por uso de datos biométricos

15. ¿Te preocuparía el uso de datos biométricos para acceder a sistemas universitarios?



La siguiente tabla muestra la síntesis de los indicadores claves de la encuesta, relacionando las preguntas que tienen correlación directa con los objetivos del proyecto y a la pregunta de investigación

Tabla 9

Síntesis de indicadores claves de la encuesta

Indicador	n	%	Interpretación
Han olvidado la contraseña de SAP (al menos 1 vez)	75	86,2%	Alta incidencia de olvidos de credencial
Han tenido bloqueos de cuenta en SAP	51	58,6%	Más de la mitad ha experimentado bloqueos
El cambio periódico afecta su experiencia (leve o significativa)	72	82,8%	Impacto generalizado de la política de contraseñas
Usan biometría en dispositivos personales	82	94,3%	Altísima familiaridad previa con el mecanismo
Cómodos usando Face ID en SAP	78	89,7%	Fuerte disposición a adoptar la solución propuesta

Creen que eliminar contraseñas mejoraría su experiencia	72	82,8%	Alta valoración del impacto esperado
Viabilidad percibida (media sobre 10)	—	8,46/10	Percepción muy favorable de implementación
No les preocupa el uso de datos biométricos	48	55,2%	Mayoría no presenta barreras de privacidad

Resultados del Prototipo (componente tecnológico)

El Prototipo fue desarrollado en Python usando diferentes bibliotecas MTCNN (Multitask Cascaded Convolutional Networks) método para hacer la detección de rostros como la alineación de puntos de referencia faciales en un solo proceso, y también InceptionResnetV1 (facenet_pytorch) para la detección y codificación facial, junto con un clasificador SVM (scikit-learn) para hacer la identificación de la identidad. Se evaluó el sistema en varias oportunidades teniendo en cuenta diferentes condiciones de iluminación y de distancia entre el dispositivo y el usuario para verificar su funcionamiento

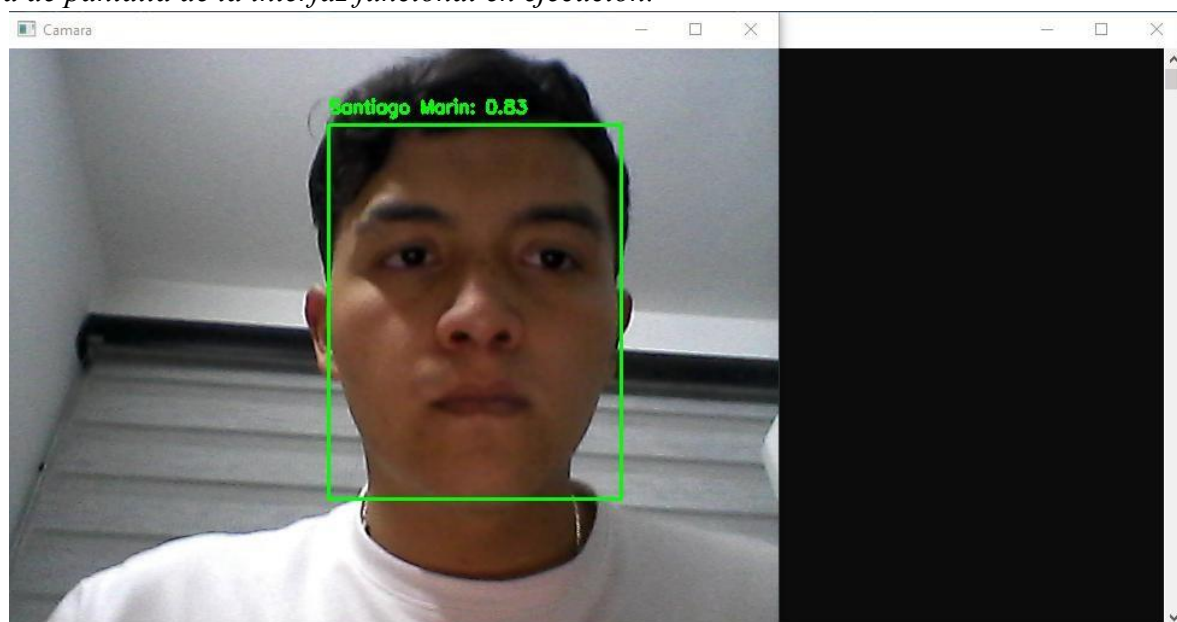
A continuación, se presenta un video demostrativo del funcionamiento del script ejecutable desarrollado para el prototipo de reconocimiento facial e integración con SAP. En el video se evidencia el proceso de autenticación biométrica, la validación del usuario y la ejecución del sistema desde la terminal de comandos (CMD), mostrando el comportamiento general de la aplicación y su funcionamiento operativo.

Enlace 1: [Video demostrativo del prototipo](#)

Adicionalmente, a continuación, se presentan una captura de pantalla de la interfaz funcional del prototipo, donde se pueden observar las pruebas de reconocimiento facial y resultados obtenidos durante la ejecución del sistema.

Ilustración 7

Captura de pantalla de la interfaz funcional en ejecución.

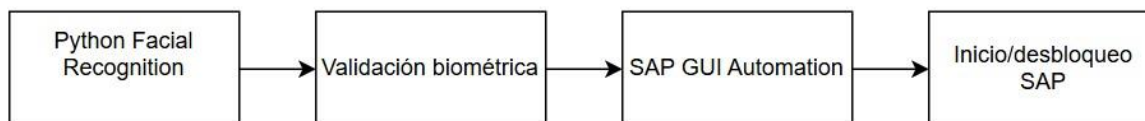


Flujo de login funcional:

Actualmente, el proyecto es únicamente un prototipo; sin embargo, su diseño está pensado para una integración directa con SAP. Dicha integración no es posible realizarla en este momento, puesto que se requiere acceso directo al sistema SAP y a un ambiente de pruebas. Debido a que, por el momento, el proyecto se encuentra en fase de prototipo, dicho acceso aún no ha sido otorgado. No obstante, a continuación, se presenta el flujo lógico del proceso de inicio de sesión (login).

Ilustración 8

Flujo login



SAP GUI es la interfaz gráfica oficial utilizada para acceder y trabajar con los sistemas SAP desde un computador. Esta herramienta permite a los usuarios interactuar con los diferentes módulos y funcionalidades de SAP mediante ventanas, formularios, transacciones y menús, facilitando la ejecución de procesos empresariales como gestión financiera, recursos humanos, logística, inventarios y administración de datos. Además, SAP GUI permite la automatización de tareas mediante funcionalidades como SAP GUI Scripting, lo que posibilita la integración con aplicaciones externas y el desarrollo de soluciones personalizadas, como sistemas de autenticación biométrica o automatización de procesos empresariales.

Las pruebas mostraron que el sistema reconoce de manera satisfactoria a los usuarios registrados, con tiempos de respuesta menores a 1,5 segundos desde la captura del frame o fotograma hasta posteriormente su visualización en pantalla, el prototipo mostro ser eficiente ante diferentes variaciones de iluminación y ángulo facial.

Estos resultados técnicos nos permiten confirmar que el desarrollo de un sistema de autenticación mediante reconocimiento facial funcional es viable con herramientas de código abierto en Python.

Discusión

Teniendo en cuenta la investigación anterior, este apartado se enfoca en revisar los resultados de este proyecto, lo que se sabía desde el principio y más llama la atención no es que los estudiantes tengan problemas con la contraseña de SAP, sino el tamaño del problema según los resultados el 86% de los estudiantes encuestados haya olvidado su clave al menos una vez y que más de la mitad haya bloqueado su cuenta, esto , muestra que el modelo implementado actualmente no es el mejor o no está funcionando bien.

Según los artículos consultados, Ometov et al. (2020) ya planteaban que los sistemas basados únicamente en contraseñas tienen limitaciones estructurales que se agravan cuando los usuarios manejan múltiples plataformas con credenciales distintas. Por otro lado, la investigación de Whitman y Mattord (2021) va un paso más allá y señalan que las políticas de renovación periódica de contraseñas, aunque están pensadas para mejorar la seguridad, terminan generando el efecto contrario: más errores, más olvidos y más carga operativa para los equipos de soporte. En el contexto de la EAN, esos mismos efectos se evidencian, en lo que les sucede a los estudiantes al momento de autenticarse en la plataforma de SAP para realizar pagos de matrículas, consultar notas, promedios, solicitar certificados entre otros.

Un dato a tener en cuenta fue el cruce entre bloqueos y satisfacción de los estudiantes al usar SAP ya que los estudiantes que han sufrido bloqueos de cuenta calificaron su experiencia de inicio de sesión con una media 3 sobre 5; por otro lado, los que nunca han bloqueado el sistema calificaron su experiencia con una puntuación de 4. Esta diferencia de un punto significa que el bloqueo no es solo un inconveniente técnico, sino que es algo que

deteriora la percepción del estudiante sobre el sistema de SAP cuando necesitan realizar procesos críticos dentro de ella.

Cataldo et al. (2022) documentaron algo similar al estudiar la satisfacción post-implementación de sistemas SAP-ERP: los usuarios valoran más los atributos que reducen el esfuerzo operativo que los que refuerzan controles de seguridad que no perciben como una amenaza directa. Dicho de otra forma, a los estudiantes no les preocupa tanto que alguien hackee su cuenta de SAP; les preocupa no poder entrar cuando lo necesitan. Y eso es exactamente lo que este proyecto busca resolver.

Al preguntarle a los estudiantes sobre las ventajas de implementar biometría para acceder a SAP, el 42 % respondió que la mayor ventaja sería el acceso más rápido. La seguridad quedó en último lugar, con solo el 9 %. Esto podría interpretarse como una falta de conciencia sobre la importancia de la seguridad de los datos sensibles, sin embargo, se podría interpretar de otra manera y es que los estudiantes no están ignorando la seguridad, simplemente están priorizando lo que más les afecta al momento de autenticarse y es la dificultad operativa de gestionar contraseñas que vencen y se olvidan en periodos cortos de tiempo.

Uno de los factores que más facilita la propuesta es que el 89 % de los estudiantes ya usa reconocimiento facial o huella dactilar en su celular o computador. Este proyecto no propone a los estudiantes que adopten algo desconocido; si no que lleven algo que ya hacen todos los días a una plataforma que también usan regularmente. Rukhiran et al. (2023) encontraron en su estudio sobre biometría en educación superior que el reconocimiento facial

fue la modalidad con mayor aceptación precisamente en entornos donde los usuarios ya tenían experiencia previa con la tecnología en dispositivos cotidianos. Este proyecto llega al mismo resultado desde otro ángulo.

No se puede ignorar que quienes ya escanean su cara para desbloquear el teléfono varias veces al día no perciben la biometría como algo intrusivo. Sí hay un 16 % que respondió "tal vez", no se puede ignorar. Jain et al. (2004) son claros al señalar que los datos biométricos tienen una característica que los hace especialmente sensibles: no pueden cambiarse si se comprometen. Por eso el diseño del prototipo no almacena imágenes fotográficas, solo vectores matemáticos que no permiten reconstruir el rostro original. Si algún día esto escala a una implementación real, ese principio de privacidad desde el diseño tendría que mantenerse.

Los resultados de este proyecto dejan en evidencia que existen problemas reales a los que se enfrentan los estudiantes al momento de autenticarse en SAP y que hay una tecnología como es el Face ID para abordarlo y hay disposición de los estudiantes para adoptarla en su proceso de autenticación. También es importante mencionar este prototipo se evaluó en condiciones controladas y con pocos usuarios, lo que no permite evaluar el comportamiento del sistema a una gran escala como es la institucional, Hossain y Muhammad (2020) advierten sobre los retos de escalabilidad en sistemas biométricos en entornos distribuidos. Esta sería una oportunidad de mejora si se llega a implementar, queda claro que la solución es técnicamente alcanzable con herramientas de código abierto y accesibles, sin necesidad de infraestructura costosa.

Plan de Divulgación

Este plan de divulgación tiene como objetivo definir cómo se presentarán los resultados del proyecto de grado el cual es “Diseño de un prototipo funcional de un sistema de Autenticación Biométrica basado en Reconocimiento facial para el acceso a SAP en la universidad EAN” mediante diferentes estrategias que permitan su visibilidad, validación y posible aplicación en entornos reales, la siguiente tabla muestra el plan de divulgación propuesto.

Tabla 10

Plan de divulgación

Elemento	Descripción
Producto principal	Artículo científico más el código fuente sobre autenticación biométrica en el entorno de las universidades de educación superior
Medio de divulgación	Repositorio institucional para el artículo y el código fuente en un repositorio de GitHub bajo licencia de código abierto.
Estrategias	Realizar correcciones de artículo, elaboración de presentación mostrando los principales resultados del análisis para socializarlo en eventos académicos
Cronograma	1 mes posterior a la finalización del proyecto
Recursos	Acompañamiento de la tutora de Proyecto de Integración, acceso a plataformas institucionales, herramientas de desarrollo

Aliados	Grupos de investigación, semilleros, comunidad académica, Facultad de Ingeniería de la universidad EAN.
Resultados esperados	Visibilidad del proyecto, para documentar un caso de implementación de autenticación en el contexto universitario, validación académica ya que a mediano plazo los resultados podrían servir para que la dirección de Tecnología de la EAN evalúe la posibilidad de un piloto real.

Conclusiones

Tras pasar por diferentes etapas primero con la investigación analizando diferentes perspectivas de autores con respecto a una implementación de Face ID, y por otro lado obtener y analizar los resultados cuantitativos de la encuesta donde los estudiantes presentaban su opinión sobre el acceso a SAP, el desarrollo del proyecto permitió cumplir con los cuatro objetivos específicos que se plantearon y obtener respuestas a la pregunta de investigación y las hipótesis

1. Analizar las dificultades que enfrentan los estudiantes en la gestión de contraseñas en el sistema SAP: El análisis de los 87 estudiantes a los cuales se les aplicó la encuesta confirmó que el 86% de veces ha olvidado la contraseña al menos una vez y el 59% ha bloqueado la cuenta al momento de autenticarse. Al correlacionar satisfacción y bloqueo de cuenta se infiere que los estudiantes con bloqueos de cuenta calificaron la experiencia con una media de 3 sobre 5 frente a una de 4 de quienes no lo han tenido. Estos resultados validan la hipótesis 2 de que la frecuencia de bloqueos y solicitudes de recuperación de contraseñas en SAP es significativa y está vinculada a la insatisfacción de los estudiantes con el sistema actual
2. Evaluar la viabilidad técnica de las tecnologías de autenticación biométrica basadas en reconocimiento facial, ya que la revisión de artículos científicos con la metodología prisma permitió confirmar que las tecnologías basadas en reconocimiento facial basadas en modelos de aprendizaje profundo como FaceNet e InceptionResnetV1 son compatibles con hardware convencional respaldando la viabilidad técnica de la solución propuesta en el entorno universitario.

3. Desarrollar un prototipo funcional de inicio de sesión biométrica utilizando reconocimiento facial, mediante el lenguaje de programación Python y librerías especializadas: El prototipo diseñado en Python integrado con MTCNN para la detección facial, InceptionResnetV1 para generación de embeddings y un clasificador SVM para la identificación operó en los dispositivos personales de los usuarios que probaron el sistema
4. Validar la aceptación del prototipo desarrollado mediante pruebas de usabilidad con estudiantes de la EAN evaluando indicadores como tiempo de acceso, facilidad de uso, nivel de satisfacción y percepción frente al sistemas: El 90% de los estudiantes encuestados se mostro cómodo con el uso de Face Id en SAP y el 83% considero que un sistema de autenticación sin contraseñas mejoraría su experiencia de acceso, confirmando la hipótesis 1, la cual menciona que la implementación de autenticación biométrica mejoraría su experiencia de acceso medida a través de la facilidad percibida y el nivel de satisfacción de los estudiantes.

Algunas de las limitaciones evidenciadas son, primero que el muestreo no probabilístico no permite obtener estadísticas de los resultados a toda la población de la EAN y por otro lado el prototipo fue evaluado bajo condiciones controladas con pocos usuarios lo que no permite evidenciar como se comportaría el sistema a gran escala. Estas limitaciones no invalidan los resultados obtenidos, pero delimitan el alcance de las conclusiones a un ámbito de viabilidad exploratoria.

Referencias

Ávila-Coello, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. *Journal of Economic and Social Science Research*, 4(2), 140–156. <https://doi.org/10.55813/gaea/jessr/v4/n2/> 96

Aznarte, J. L., Melendo Pardos, M., & Lacruz López, J. M. (2022). Sobre el uso de tecnologías de reconocimiento facial en la universidad: el caso de la UNED. *RIED. Revista Iberoamericana de Educación a Distancia*, 25(1), 261-277.
<https://doi.org/10.5944/ried.25.1.31533>

Badman, A., & Kosinski, M. (2025, noviembre 28). ¿Qué son los datos? *Ibm.com*.
<https://www.ibm.com/es-es/think/topics/data>

Bergmann, D. (2025, noviembre 27). ¿Qué es el machine learning? IBM Think.
<https://www.ibm.com/es-es/think/topics/machine-learning>

Cataldo, A., Bravo-Adasme, N., Lara, A. M., & Rojas, J. (2022). Factors influencing the post-implementation user satisfaction of SAP-ERPS. *INGENIARE — Revista Chilena de Ingeniería*, 30(3), 574–591.

Hossain, M. S., & Muhammad, G. (2020). Cloud-assisted secure biometric authentication for mobile Internet of Things. *Future Generation Computer Systems*, 108, 507–518. <https://doi.org/10.1016/j.future.2020.02.012>

IDEMIA obtiene el premio de la Security Industry Association (SIA) al mejor producto biométrico gracias a VisionPass, su dispositivo de reconocimiento facial avanzado. (2020, Jul 15). Business Wire En Español

<https://login.bdbiblioteca.universidadean.edu.co/login?url=https://www-proquest-com.bdbiblioteca.universidadean.edu.co/wire-feeds/idemia-obtiene-el-premio-de-la-security-industry/docview/2423785550/se-2>

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4–20. <https://doi.org/10.1109/TCSVT.2003.818349>

LUICON. (2018). Lo que se puede hacer hoy con la autenticación biométrica en Colombia. *Portafolio*. <https://www-proquest-com.bdbiblioteca.universidadean.edu.co/trade-journals/lo-que-se-puede-hacer-hoy/docview/1986604909/se-2>

Morales, A., Fierrez, J., Tolosana, R., Vera-Rodríguez, R., & Bartolomé, I. (2015). Biometric student authentication for e-learning platforms. *Computers & Security*, 52, 1–12. <https://doi.org/10.1016/j.cose.2015.03.001>

MetaFlip. (s/f). Edu.co. Recuperado el 8 de marzo de 2026, de <https://repositorio.uniandes.edu.co/flip/?pdf=/bitstreams/a6c98c0e-633c-4c38-93ed-2e55cbda0559/download>

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2020). Multi-factor authentication: A survey. *Cryptography*, 2(1), 1–31.
<https://doi.org/10.3390/cryptography2010001>

Rukhiran, M., Wong-In, S., & Netinant, P. (2023). IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach. *IEEE Access*, 11, 22767–22787. <https://doi.org/10.1109/ACCESS.2023.3253592>

SAP SE. (2021). *SAP S/4HANA overview*. <https://www.sap.com/products/s4hana-erp.html>

SAP. (2023). *SAP Single Sign-On: Secure access to business applications*.
<https://www.sap.com/products/financial-management/single-sign-on-solution.html>

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 815–823).
<https://doi.org/10.1109/CVPR.2015.7298682>

SecurityBridge. (2025, July 23). *SecurityBridge adquiere CyberSafe para ofrecer SSO contextual, MFA y autenticación sin contraseña a los usuarios de SAP*. Business Wire.
<https://www.proquest.com/>

Shen, L., Lin, Z., Huang, Q., & Li, H. (2022). Face recognition-based authentication system using deep learning techniques. *IEEE Access*, 10, 53421–53432.
<https://doi.org/10.1109/ACCESS.2022.3172145>

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*, 3(5), 637–646.
<https://doi.org/10.1109/jiot.2016.2579198>

Wang, M., Deng, W., Hu, J., Tao, X., & Huang, Y. (2021). Deep learning for face recognition: A survey. *Pattern Recognition*, 110, 107547.
<https://doi.org/10.1016/j.patcog.2020.107547>

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.