UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

ESCUELA DE POSTGRADO

PROGRAMA DE MAESTRÍA EN CIBERSEGURIDAD Y GESTIÓN DE LA INFORMACIÓN

Modelo de autenticación biométrica fisiológica o conductual para prevenir intrusiones usando Zero trust para Arquitecturas Cloud

TRABAJO DE INVESTIGACIÓN

Presentado como parte de los requisitos para optar el grado académico de Maestro en Ciberseguridad y Gestión de la Información

AUTOR(ES)

Quispe Cieza, Francisco	0000-0002-0166-2730
Lipa Maza, Barnabi Jhon	0000-0002-7700-3336
Palao Cahuana, Juan Nestor	0000-0002-1076-355X

ASESOR(ES)

Campos Cabrera, Carlos Enrique	0000-0003-4020-4748

Lima, 26 de enero de 2024

Dedicatoria

Dedicamos este trabajo, en primer lugar, a Dios.
También a nuestros familiares y docentes,
por apoyarnos día a día a crear este aporte con nuestra investigación y seguir adelante.

Agradecimientos

En primer lugar, damos gracias a Dios y a nuestros padres, quienes nos brindaron todo su apoyo para cumplir nuestros sueños. Además, queremos expresar nuestro más profundo agradecimiento a esta casa de estudios, por habernos formado con un grupo de docentes cualificados. Finalmente, queremos agradecer al director de la maestría y a nuestro asesor, quienes nos brindaron su apoyo durante todo nuestro proceso de investigación.

Resumen

La transformación digital a la nube ha generado preocupación por nuevas necesidades de seguridad. Las amenazas en ciberseguridad tienen una amplia gama de ataques o intrusiones. Los atacantes o piratas informáticos pueden eludir la gestión de privilegios, el uso de VPN (virtual private network), firewalls e IDS (intrusion detection systems) mediante técnicas como el phishing, suplantación de identidad y ataques de día cero. Según el reporte de ESET 2022, en Latinoamérica la principal preocupación sigue siendo la infección con códigos maliciosos (66 %), robo de información (62 %) y accesos indebidos a sistemas (59 %). Una vez los atacantes hayan accedido con una identidad legítima o camuflada a un sistema ya sea Cloud u on-premise, el entorno los considera confiables. Esta brecha tecnológica llevó a niveles elevados el robo de información y la suplantación de identidad. El documento tiene como primer objetivo proporcionar una revisión de los sensores biométricos fisiológicos y conductuales para mejorar la autenticación biométrica.

La investigación propone un modelo de autenticación biométrica fisiológica o conductual que prevenga intrusiones usando Zero Trust para arquitecturas Cloud. Lo que se aborda en la investigación es que el usuario se autentica utilizando una característica biométrica conductual o fisiológica, como el patrón de escritura o el reconocimiento facial o iris. Los datos biométricos se envían a una nube segura para su procesamiento y verificación, la nube verifica la autenticación del usuario utilizando una política de Zero Trust que establece que todas las solicitudes de acceso deben ser autenticadas y autorizadas antes de ser aceptadas. Si la autenticación del usuario es válida, se le otorga acceso a los recursos y se registra como actividad segura dentro del Identity Provider. Si la autenticación del usuario es inválida o sospechosa, se le niega el acceso y se registra como una intrusión dentro del Identity Provider. Este modelo de autenticación biométrica, con enfoque de Zero Trust para arquitecturas Cloud, proporciona un alto nivel de seguridad y protección contra intrusiones, ya que combina la verificación biométrica con la protección del modelo Zero Trust y el procesamiento seguro en la nube para proteger la integridad, la disponibilidad y la confidencialidad.

Palabras clave: Control de acceso; autenticación; vulnerabilidades; biometría conductual; biométrica fisiológica; Cloud; Zero Trust.

Abstract

Digital transformation to Cloud has generated concern about new security needs; cybersecurity threats have a wide range of attacks or intrusions. Attackers or hackers can bypass privilege management, the use of VPN (virtual private network), firewalls, IDS (intrusion detection systems) with techniques such as phishing, spoofing, and zero-day attacks. According to the ESET 2022 report, in Latin America the main concern continues to be infection with malicious codes (66%), information theft (62%) and improper access to systems (59%). Once attackers have accessed a system, whether Cloud or on-premise, with a legitimate or camouflaged identity, the environment considers them trustworthy. This technological gap led to high levels of information theft and identity theft. The paper first aims to provide a review of physiological and behavioral biometric sensors to improve biometric authentication.

The research proposes a physiological or behavioral biometric authentication model that prevents intrusions using Zero trust for Cloud architectures. What is addressed in the research is that; the user is authenticated using a behavioral or physiological biometric characteristic, such as writing pattern or facial or iris recognition. Biometric data is sent to a secure cloud for processing and verification, the cloud verifies user authentication using a Zero Trust policy, which states that all access requests must be authenticated and authorized before being accepted. If the user's authentication is valid, they are granted access to the resources and logged as secure activity within the Identity Provider. If the user's authentication is invalid or suspicious, access is denied and is logged as an intrusion within the Identity Provider. This biometric authentication model, with a Zero Trust approach for Cloud architectures, provides a high level of security and protection against intrusions; as it combines biometric verification with Zero Trust model protection and secure cloud processing to protect integrity, availability, and confidentiality.

Keywords: Access control; authentication; vulnerabilities; behavioral biometrics; physiological biometrics; Cloud; Zero Trust.

e202110210_Quispe Cieza, Francisco_Modelo de autenticación biométrica fisiológica o conductual para prevenir intrusiones usando Zero trust para Arquitecturas Cloud

INFORME DE ORIGINALIDAD

17%	17%	9%	11%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	upc.aws.openrepository.com Fuente de Internet	2%
2	repositorioacademico.upc.edu.pe Fuente de Internet	1%
3	dspace.ucuenca.edu.ec Fuente de Internet	1%
4	hernandez.gearslite.info Fuente de Internet	1%
5	www.informatica-juridica.com Fuente de Internet	1%
6	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%
7	www.pmg-ssi.com Fuente de Internet	1%

hdl.handle.net

Índice de contenidos

1. Problemática 1

1.1 Antecedentes 1

1.2 Planteamiento del problema 3

1.3 Objetivo general 4

1.4 Objetivos específicos 4

1.5 Alcance y limitaciones 4

1.6 Justificación y viabilidad 4

2. Marco conceptual 6

2.1 Introducción 6

2.2 Conceptos 6

2.2.1 Arquitectura Cloud. 6

2.2.2 Autenticación biométrica 8

2.2.3 Arquitectura Zero Trust. 10

2.3 Marco regulatorio 12

2.3.1 Ley de Protección de Datos Personales. 12

2.3.2 Ley de Firmas y Certificados Digitales. 13

2.4 Buenas prácticas 13

2.4.1 ISO 27001. 14

2.4.2 ISO 27002 – 2013. 15

2.4.3 ISO 27017. 16

2.4.4 ISO 27033-4. 16

2.4.5 ISO 22301. 17

2.4.6 ISO 24761. 17

2.4.7 ISO 19794-6. 18

2.4.8 NIST. 18

2.4.8.1 NIST SP 800-76-2. 19

2.4.8.2 NIST SP 800-145. 19

2.4.8.3 NIST SP 800-207. 20

3. Estado del arte 21

3.1 Introducción 21
3.2 Revisión sistemática de la literatura 21
3.2.1 Búsqueda de palabras clave. 21
3.2.2 Preguntas de investigación. 23
3.2.3 Estrategia y procesos de búsqueda. 24
3.3 Metodología 27
3.4 Planificación 28
3.4.1 Preguntas de investigación. 28
3.4.2 Bancos. 28
3.4.3 Palabras claves. 28
3.4.4 Periodo. 28
3.4.5 Criterios de inclusión y exclusión. 29
3.5 Desarrollo 29
3.6 Resultados 49

4. Proceso para el desarrollo del artefacto 51

4.1 Metodología de la Investigación 51
4.1.1 Tipo y diseño de la investigación. 51
4.1.2 Hoja de ruta para el desarrollo del artefacto. 51
4.1.3 Plan de trabajo. 52
4.2 Análisis de la solución 53
4.2.1 Análisis de sensores biométricos para prevenir intrusiones, en conformidad con la Ley de Protección de Datos Personales (LPDP N.° 29733) y la Organización Internacional de Normalización (ISO 27001) en arquitecturas Cloud. 54
4.2.2 Análisis de los sensores biométricos a través de métricas. 56
4.2.3 Análisis biométrico del tipo reconocimiento facial y de Iris según la FRVT e ICE de NIST. 60
4.2.4 Análisis de la de la Ley de Protección de datos Personales 29733 y el SGSI de la ISO 27001. 63
4.2.5 Pilares del SGSI ISO 27001 para las arquitecturas Cloud. 66
4.3 Alcance de la solución 71
4.4 Diseño de la solución 71
4.4.1 Arquitectura Cloud. 73

4.4.2 Arquitectura biométrica 73
4.4.3 Construcción de la solución. 73
4.4.4 Enfoques de acceso. 75
4.4.5 Procesos de autenticación y autorización propuestos. 75

5. Desarrollo del artefacto 79

5.1.1 Diagnóstico resultante. 79

6. Protocolo de validación 82

6.1 Análisis de riesgos 82
6.2 Modelo de madurez 87
6.3 Plan de implementación 93
6.4 Trabajos futuros 95

Conclusiones 97

Recomendaciones 99

Glosario 101

Referencias 109

Anexos 115

Anexo 1. 115

Implementación de la solución propuesta 115

Lista de tablas

Tabla 1 Justificación y viabilidad 5
Tabla 2 Ciclo de Deming - PDCA 14
Tabla 3 Búsqueda de palabras clave 22
Tabla 4 Selección de las palabras clave 22
Tabla 5 Preguntas de investigación 23
Tabla 6 PICOC de la pregunta 1 24
Tabla 7 PICOC de la pregunta 2 25
Tabla 8 PICOC de la pregunta 3 26
Tabla 9 PICOC de la pregunta 4 27
Tabla 10 Criterios de inclusión y exclusión 29
Tabla 11 Artículos científicos seleccionados para el estudio 29
Tabla 12 Artículos científicos seleccionados para el estudio 31
Tabla 13 Investigaciones por tipo de contribución 50
Tabla 14 Análisis de sensores biométricos fisiológicos y conductuales 57
Tabla 15 *Definición de criterios y niveles para las métricas* 58
Tabla 16 *Resumen de los sistemas de autenticación biométrica existentes con características estáticas* 59
Tabla 17 *Face Recognition Vendor Test (FRVT)* 60
Tabla 18 *Análisis del impacto de la biometría fisiológica y conductual en función los papers revisados dentro del Q1-Q2 para nuestra investigación* 61
Tabla 19 *Métricas para la valorización de la precisión, eficiencia, usabilidad, seguridad, privacidad.* 62
Tabla 20 *Principios de la Ley de Protección de datos Personales 29733 y el SGSI de la ISO 27001* 63
Tabla 21 *Pilares del SGSI ISO 27001 para las arquitecturas Cloud* 66
Tabla 20 *Componentes ero trust para el modelo de autenticación propuesto* 80
Tabla 21 *Controles asociados a la ISO 27001-2* 83
Tabla 22 *Tratamiento del Riesgo con la Norma ISO 27001-2* 86
Tabla 23 *Análisis del impacto de la biometría fisiológica o conductual en función a papers que se encuentran dentro del Q1-Q2 para nuestra investigación.* 87
Tabla 24 *Face Recognition Vendor Tes (FRVT)* 88

Tabla 25 *Seguridad en la integración de la arquitectura Biométrica, Cloud, Zero Trust para los tres pilares del SGCI: Integridad, Disponibilidad y Confidencialidad* 88
Tabla 26 89
Tabla 27 *Nivel de madurez para el método de autenticación biométrica fisiológica o conductual para prevenir intrusiones en una arquitectura Cloud* 90
Tabla 28 *Visibilidad en la norma ISO 22301 para la integración de la continuidad del negocio en la planificación estratégica y operativa de la organización: User Authentication on Mobile Device* 92
Tabla 29 *Visibilidad en la norma ISO 22301 para la integración de la continuidad del negocio en la planificación estratégica y operativa de la organización: Authentication Techniques* 92
Tabla 30 *Plan de implementación* 93

Lista de figuras

Figura 1 Reporte de las principales intrusiones en América Latina en temas de seguridad. 1
Figura 2 Reporte de los países más afectados con de códigos maliciosos 2
Figura 3 Ranking de los ataques en las industrias 3
Figura 4 Arquitectura Cloud Computing 6
Figura 5 Tipos de servicios Cloud la arquitectura Cloud 8
Figura 6 Arquitectura de un sistema biométrico para identificación personal con huellas dactilares 10
Figura 7 Componentes lógicos básicos de Zero Trust 11
Figura 8 Marco de Ciberseguridad del NIST 19
Figura 9 Diagrama de Ven 23
Figura 10 Diagrama de la metodología s 51
Figura 11 Diagrama Diseño de la construcción del artefacto 52
Figura 12 Plan de trabajo 53
Figura 13 Categorías de autenticación de usuarios 53
Figura 14. Sensores biométricos a través de métricas 56
Figura 15 Safety in Cloud Computing 72
Figura 16 Arquitectura Cloud - En función a la ISO 27001-2 para el control de riesgos criterios 73
Figura 17 Arquitectura Biométrica - En función a las buenas prácticas de a ISO 24761 .. 73
Figura 18 Proceso de autenticación propuesto 77
Figura 19 Proceso de autorización propuesto 78
Figura 20 Constructor 79
Figura 21 Artefacto 81
Figura 22 Nivel de madurez de la biometría fisiológica 90
Figura 23 Nivel de madurez de la biometría conductual 91
Figura 24 Reporte de Vulnerabilidades 115
Figura 25 Página Web en Plataforma Google Cloud 116
Figura 26 Instancia de la página Web 116
Figura 27 Acceso a la página Web 116
Figura 28 API Identity Aware Proxy 117
Figura 29 Uso del protocolo 117

Figura 30 Configuración del uso del API 118
Figura 31 Habilitar el API para el uso en APP Engine 118
Figura 32 Prueba de acceso a la página Web 119
Figura 33 Autenticación no permita 120
Figura 34 Autenticación no permita 121
Figura 35 Software Microsoft Authenticator 122
Figura 36 Selección de cuenta de correo 122
Figura 37 Software Microsoft Authenticator 123
Figura 38 Ventana de bienvenida después de la autenticación satisfactoria 123

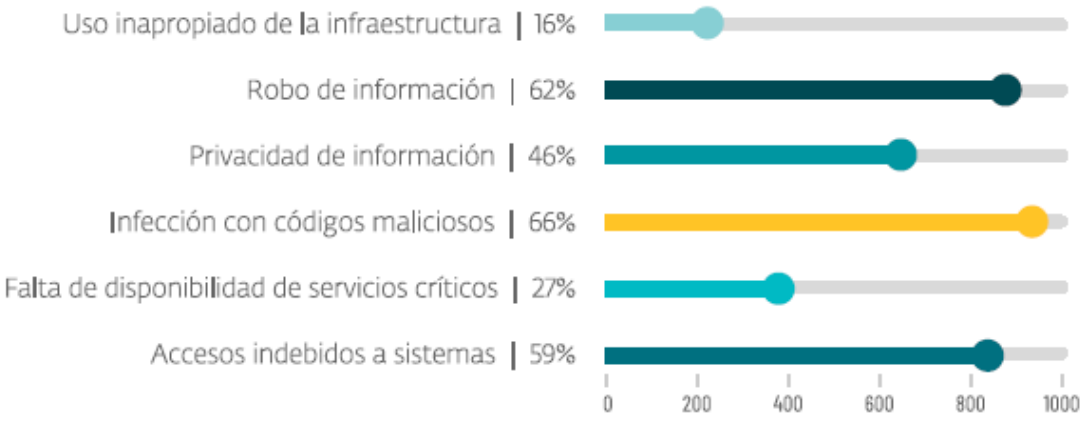
1. Problemática

1.1 Antecedentes

Según ESET (2022), en Latinoamérica la principal preocupación sigue siendo la infección con códigos maliciosos (66%), robo de información (62%) y accesos indebidos a sistemas (59%).

Figura 1

Reporte de las principales intrusiones en América Latina en temas de seguridad

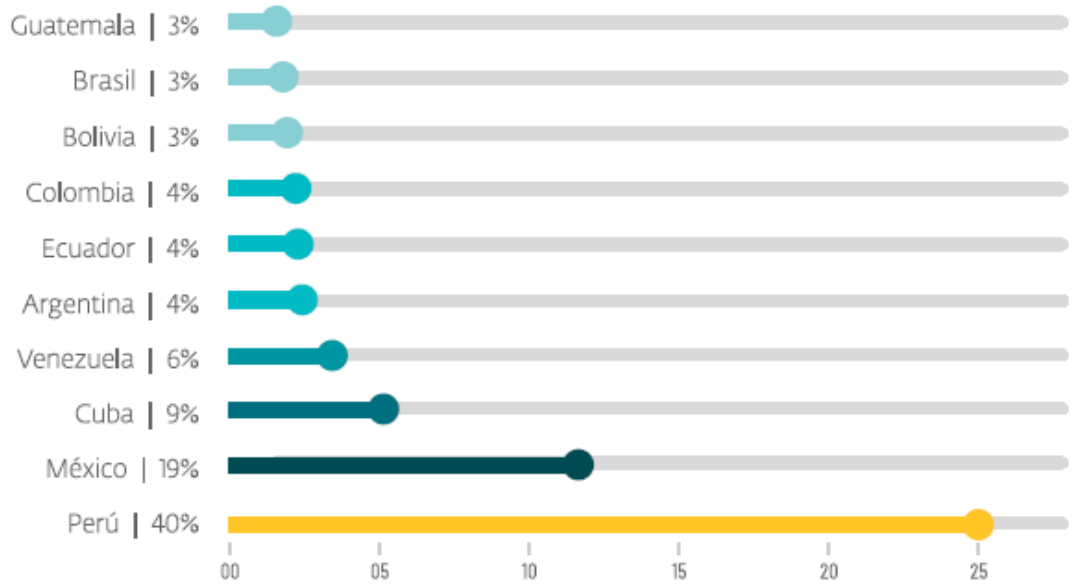


Nota. Principales preocupaciones de las empresas en América Latina en temas de seguridad. De "Security Report Latinoamérica 2022", por ESET, 2022 (https://www.eset.com/ve/security-report/).

Según los datos de la telemetría, el país más afectado por la categoría de códigos malicioso es Perú, con el 40% de las detecciones. ESET, (2022)

Figura 2

Reporte de los países más afectados con de códigos maliciosos



Nota. Países con mayores detecciones de códigos maliciosos. De "Security Report Latinoamérica 2022", por ESET, 2022 (https://www.eset.com/ve/security-report/).

Por otro lado, International Business Machines (IBM, 2022), en su reporte X-Force Threat Intelligence Index, señala que el phishing fue el vector de infección más común que los actores de amenazas utilizaron contra los objetivos de América Latina; y representó el 47 % de los ataques que X-Force detectó en esta región. La gran cantidad de ataques BEC (compromiso de correo electrónico empresarial) y ataques de Ransomware, entregados a través de phishing probablemente esté impulsando esta tendencia. Las credenciales robadas provocaron el 29 % de los ataques a organizaciones latinoamericanas, y este alto porcentaje en comparación con otras regiones sugiere que un uso más generalizado de MFA podría ayudar a reducir los incidentes de credenciales robadas y BEC en Latinoamérica. La explotación de vulnerabilidades generó solo el 18 % de los incidentes en las organizaciones latinoamericanas, mientras que los medios extraíbles representaron otro 6 %.

La industria manufacturera fue la del mayor objetivo en América Latina en 2021, pero con un 22 %, retail (20 %), finanzas y seguros (15 %) y, quizás lo más sorprendente, la minería (11 %) (IBM, 2022).

Brasil, México y Perú fueron los países más atacados en América Latina.

Figura 3

Ranking de los ataques en las industrias

Top attacked industries

1.	Manufacturing	22%
2.	Retail and wholesale	20%
3.	Finance and insurance	15%

Nota. Top attacked industries. De "X-Force Threat Intelligence Index 2022". Por IBM, 2022. (https://www.ibm.com/downloads/cas/ADLMYLAZ)

1.2 Planteamiento del problema

¿Cómo puede un modelo de autenticación biométrica mejorar los controles de seguridad para prevenir intrusiones como vulnerabilidades que afectan la confidencialidad, disponibilidad e integridad de la información en arquitecturas Cloud?

Planteamiento de la solución

Por lo tanto, es esencial abordar este problema de manera efectiva mediante un modelo de autenticación biométrica fisiológica o conductual, respaldado por el modelo Zero Trust. Este modelo debe no solo fortalecer la autenticación de usuarios, sino también proporcionar un marco de seguridad más sólido que desafíe las suposiciones tradicionales y reduzca la exposición a riesgos. La implementación de este modelo se convierte en un imperativo para salvaguardar la integridad y confidencialidad de los datos en arquitecturas de Cloud, garantizar la disponibilidad de servicios críticos y proteger la privacidad de los usuarios en un entorno tecnológico en constante evolución.

Ante la necesidad descrita, se propone el desarrollo de un modelo de autenticación biométrica fisiológica o conductual usando el modelo Zero trust para arquitecturas Cloud. El desarrollo de este modelo se realizará a partir del análisis de tipos de sensores biométricos fisiológicos o conductuales junto con la integración del modelo Zero trust. El presente trabajo de investigación busca que las organizaciones puedan prevenir intrusiones y así poder protegerse contra ciberataques.

1.3 Objetivo general

Aplicar un modelo de autenticación biométrica fisiológica o conductual para prevenir intrusiones usando Zero Trust en arquitecturas Cloud.

1.4 Objetivos específicos

- Analizar sensores biométricos para prevenir intrusiones, en conformidad con la Ley de Protección de Datos Personales (LPDP) 29733 y la Organización Internacional de Normalización (ISO) 27001, en arquitecturas Cloud.
- Diseñar un modelo de autenticación biométrica para prevenir intrusiones usando Zero Trust para arquitecturas Cloud.
- Evaluar el modelo de autenticación biométrica para prevenir intrusiones usando Zero Trust para arquitecturas Cloud.

1.5 Alcance y limitaciones

El alcance de la propuesta será: Descriptivo

- Se justifica en el análisis realizado en la matriz del conocimiento del estado del arte.
- Describimos información básica para que los usuarios puedan comprender en qué consiste la autenticación biométrica.

1.6 Justificación y viabilidad

Para la justificación y la viabilidad se han formulado cinco lineamientos en el estudio a realizar.

Tabla 1

Justificación y viabilidad

Justificar el estudio a realizar	
Conveniencia	El modelo de autenticación biométrica propuesto permitirá mejorar la postura en ciberseguridad.
Relevancia social	Actuará como paraguas para evitar el filtro de información sensible del sector que conlleve a impactos financieros y reputacionales.
Implicaciones prácticas	Existen riesgos potenciales en el sistema biométrico, como la posibilidad de intrusiones que provocan divulgación de privacidad de la propia biometría. Estas intrusiones hacen un particular sistema expuesto al peligro. Información e intereses del usuario se ven amenazados como resultado. La información biométrica utilizada en el sistema de autenticación es parte de la privacidad del usuario, que merece una protección especial.
Valor teórico	Esta investigación permitirá controlar intrusiones en arquitecturas Cloud.
Utilidad metodológica	La implementación de un modelo de autenticación biométrica fisiológica o conductual permitirá prevenir intrusiones y mejorar la experiencia del usuario.

2. Marco conceptual

2.1 Introducción

A continuación, se detallan los conceptos teóricos que se relacionan con nuestro tema de investigación.

2.2 Conceptos

2.2.1 Arquitectura Cloud.

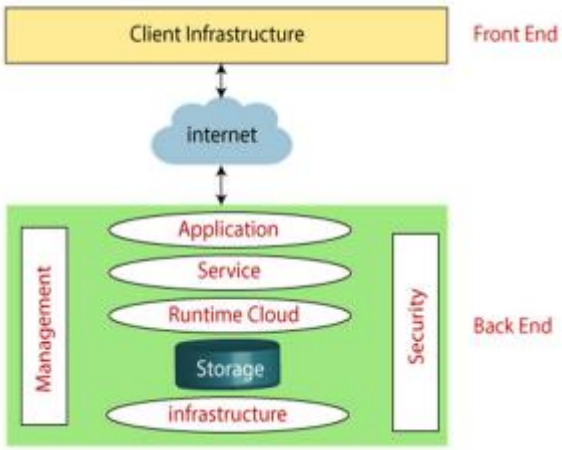
Como lo dicen Banger et al. (2022):

El término "nube" se refiere a herramientas y servicios de software que se ejecutan a través de Internet o mediante un navegador web. La computación en la nube se representa la prestación de servicios tales como almacenamiento de datos, redes y servidores a través de Internet.

La tecnología de la computación en la nube es una mezcla de una arquitectura orientada a servicios y dirigida a eventos. La arquitectura Cloud se divide en Front y Back End.

Figura 4

Arquitectura Cloud Computing



Nota. Arquitectura de computación en la nube. De “A Review Paper on Cloud Computing Architecture, Types, Advantages and Disadvantages”, por Banger et al., 2022 (https://ijarsct.co.in/Paper3144.pdf).

Como lo dicen Banger et al. (2022):

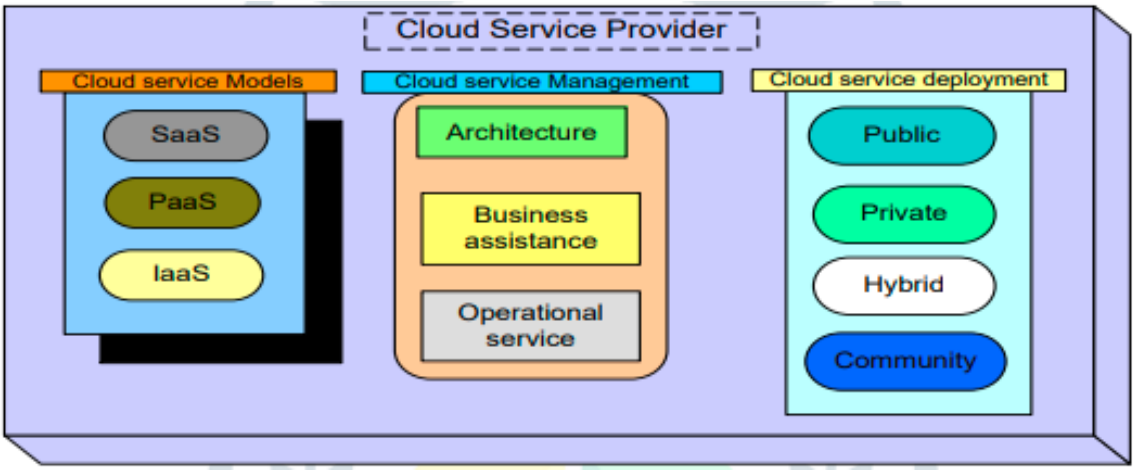
Tipos de Cloud:

- Nube pública: Esta nube se caracteriza por contar con mucho almacenamiento. Los equipos empresariales suelen utilizar una nube pública para proyectos colaborativos o desarrollo de software. Muchas plataformas también permiten a sus clientes pagar por más capacidad según sea necesario, lo que permitirá la escalabilidad.
- Nube Privada: Esta nube permite que sus usuarios accedan, usen y almacenen datos en la nube desde cualquier lugar. La infraestructura de la nube privada, por otro lado, está frecuentemente protegida por un firewall, que es un dispositivo de seguridad de la red que monitorea y restringe el tráfico de red. Las nubes privadas son preferidas por empresas con estrictos criterios regulatorios para proteger su información y datos.
- Nube Híbrida: Las nubes híbridas combinan los beneficios de las nubes públicas y privadas. Están diseñados para permitir que los consumidores usen y guarden datos en ambas plataformas al mismo tiempo.
- Nube comunitaria: Una nube privada que funciona de manera similar a una nube pública se denomina nube comunitaria. Son colaborativos en naturaleza, permitiendo a diferentes empresas autorizadas intercambiar y colaborar en las mismas aplicaciones. Las nubes comunitarias son comúnmente utilizadas por proveedores de atención médica e instituciones gubernamentales.

Tipos de Servicios Cloud

Figura 5

Tipos de servicios Cloud



Nota. Arquitectura de computación en la nube. De "Cloud Computing Architecture Issues and Future Research Directions", por Saqib et al., 2018 (https://www.jetir.org/papers/JETIRDR06081.pdf).

2.2.2 Autenticación biométrica

Como dicen Cortés Osorio et al. (2010):

> El concepto biometría por su etimología proviene de las palabras bio (vida) y metría (medida), consiste en técnicas que miden e identifican las características físicas únicas de organismos vivos o patrones de su comportamiento, que permiten identificar diferentes rasgos, por ejemplo, las huellas dactilares. (p. 98)

Como lo dice Kanak (2018):

> Los sistemas biométricos han ido mucho más allá de la autenticación local. Los avances recientes muestran que el uso de la biometría en sistemas redes distribuidas con el uso efectivo de rasgos multimodales y dispositivos móviles ha abierto una nueva puerta para las aplicaciones biométricas. La biometría se ha convertido en elementos pioneros de los servicios móviles sobre entornos de nube ya que hay un uso muy creciente de dispositivos móviles como teléfonos inteligentes, relojes inteligentes y tabletas. No solo el uso móvil, la nueva generación sistemas biométricos se centran en esquemas de seguridad avanzados

sobre redes a gran escala considerando la preservación efectiva de la privacidad, intercambio de secretos y datos seguros intercambio entre partes (pp. 510-518).

Como dicen Jangid y Bharadi (2020):

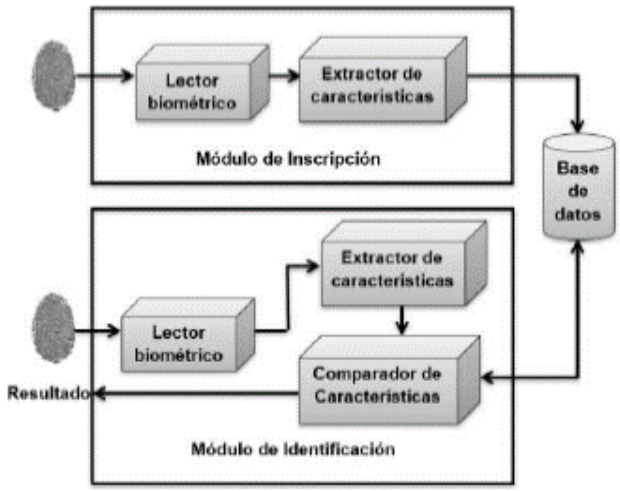
La arquitectura biométrica se basa en una serie de etapas o módulos que trabajan juntos para proporcionar un sistema de seguridad que sea eficaz y preciso. Estos módulos pueden incluir:

- Adquisición: se recopilan las características biométricas únicas de una persona utilizando sensores especializados como cámaras, escáneres de huellas dactilares o micrófonos.
- Preprocesamiento: se realiza una limpieza y mejora de las imágenes o señales biométricas para reducir el ruido y mejorar la calidad de la información.
- Extracción: se utilizan algoritmos especializados para extraer características únicas de las imágenes o señales biométricas, lo que permite la identificación y autenticación de una persona.
- Comparación: se compara la información extraída con las características biométricas almacenadas previamente en una base de datos, para verificar la identidad de la persona.
- Decisión: se toma una decisión en función de la comparación de las características biométricas, determinando si la persona es auténtica o no.

La figura 6 exhibe la estructura característica de un sistema biométrico, que se puede dividir en dos componentes principales: el módulo de enrolamiento enrollment module) y el módulo de identificación (identification module).

Figura 6

Arquitectura de un sistema biométrico para identificación personal con huellas dactilares



Nota. Diseño conceptual de un sistema biométrico para casilleros. De "Congreso Argentino de Sistemas Embebidos (CASE), 2020". (https://www.researchgate.net/publication/356541835_Diseno_conceptual_de_un_sistema_biometrico_para_casilleros)

2.2.3 Arquitectura Zero Trust.

El National Institute of Standards and Technology (NIST, 2020), en su publicación 800-207, define arquitectura Zero Trust como:

> Una arquitectura de confianza cero (ZTA) es una arquitectura de ciberseguridad empresarial que se basa en principios de confianza cero y está diseñada para evitar violaciones de datos y limitar el movimiento lateral interno. Esta publicación analiza ZTA, sus componentes lógicos, posibles escenarios de implementación y amenazas. También presenta una hoja de ruta general para las organizaciones que desean migrar a un enfoque de diseño de confianza cero y analiza las políticas federales relevantes que pueden afectar o influir en una arquitectura de confianza cero.

Algunas de las características clave de la arquitectura Zero Trust son las siguientes:

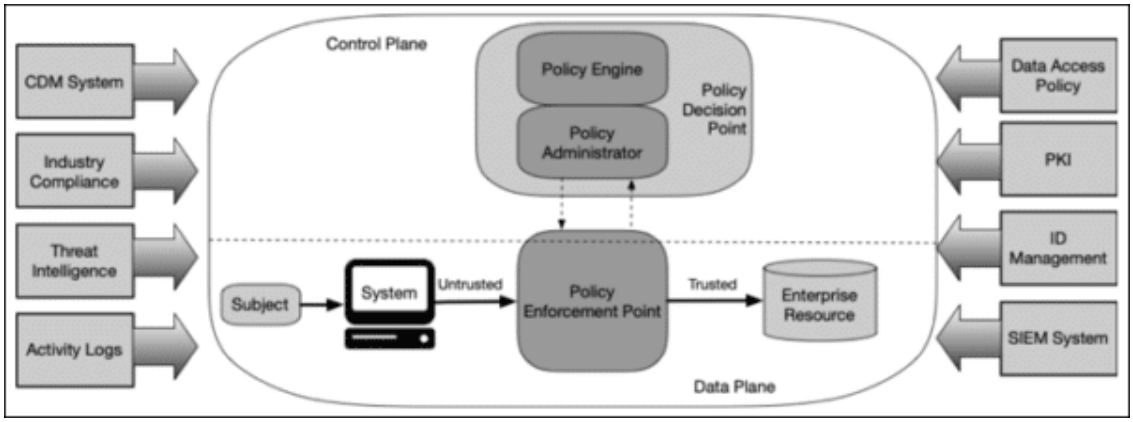
- Identidad y acceso basado en políticas: los usuarios y dispositivos deben ser autenticados y autorizados antes de que se les permita acceder a los recursos, y estas decisiones deben basarse en políticas definidas por la empresa.

- Visibilidad: la arquitectura Zero Trust requiere una visibilidad completa de los dispositivos, usuarios y aplicaciones en la red, para poder detectar y responder rápidamente a cualquier actividad sospechosa.
- Segmentación de red: la red se segmenta en partes más pequeñas y se aplican políticas de acceso estrictas entre ellas, para limitar el acceso a los recursos.
- Políticas de acceso dinámicas: las políticas de acceso se ajustan continuamente en función del comportamiento y el riesgo percibido de los usuarios y dispositivos en la red.
- Autenticación multifactorial: se requiere más de un factor de autenticación para acceder a los recursos, como una contraseña y una verificación de identidad adicional.

El diseño del modelo debe ajustarse a los recursos disponibles en una organización, así como a su apetito por el riesgo. El objetivo es aplicar un modelo de autenticación biométrica fisiológica o conductual para prevenir intrusiones en arquitecturas Cloud en escenarios de suplantación de identidad.

Figura 7

Componentes lógicos básicos de Zero Trust



Nota. De “Arquitectura Zero Trust”. Por National Institute of Standards and Technology. Special Publication 800-207, 2020. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf)

2.3 Marco regulatorio

2.3.1 Ley de Protección de Datos Personales.

> La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles. (Congreso de la República del Perú, 2013, Ley 29733, Artículo 3)

Para el tratamiento de los datos personales "se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos" (Congreso de la República del Perú, 2013, Ley 29733, Artículo 4).

El uso del tratamiento de datos debe mediar el consentimiento de su titular (Congreso de la República del Perú, 2013, Ley 29733, Artículo 5).

> Los datos personales deben ser recopilados para una finalidad determinada, explicita y licita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización. (Congreso de la República del Perú, 2013, Ley 29733, Artículo 6)

"Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados" (Congreso de la República del Perú, 2013, Ley 29733, Artículo 7).

> Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, estar actualizados, y ser necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento. (Congreso de la República del Perú, 2013, Ley 29733, Artículo 8)

"El tratamiento de los datos personales el titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales" (Congreso de la República del Perú, 2013, Ley 29733, Artículo 9).

“Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales” (Congreso de la República del Perú, 2013, Ley 29733, Artículo 10).

> Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta Ley o por los estándares internacionales en la materia. (Congreso de la República del Perú, 2013, Ley 29733, Artículo 11)
>
> La actuación de los titulares y encargados de los bancos de datos personales y, en general, de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores a que se refiere este título. Esta relación de principios rectores es enunciativa. (Congreso de la República del Perú, 2013, Ley 29733, Artículo 12)

“El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos serán tratados” (Congreso de la República del Perú, 2013, Ley 29733, Artículo 18).

2.3.2 Ley de Firmas y Certificados Digitales.

El Estado Peruano, mediante el Registro Nacional de Identificación y Estado Civil (RENIEC), es el encargado de identificar y autentificar la información que brinda un solicitante de certificado digital. Es la única entidad que lleva un registro que incluye actualmente sus datos biométricos (Reglamento de la Ley N.° 27269, Artículo 13).

Para afrontar los riesgos que puedan surgir como resultado de sus actividades de registro o verificación, el uso de la biométrica en las Entidades de Registro o Verificación acreditada debería cumplir un nivel de seguridad “Medio Alto” (Reglamento de la Ley N.° 27269, Artículo 31).

2.4 Buenas prácticas

A continuación, se detallan los conceptos teóricos que se relacionan con nuestro tema de investigación.

2.4.1 ISO 27001.

La norma ISO 27001, según ISO Tools (2019):

> Una solución de mejora continua sobre la base de la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros. Por otro lado, también permite establecer los controles y las estrategias más adecuadas para eliminar o minimizar dichos peligros. Como ocurre con todas las normas ISO, la 27001 es un sistema basado en el ciclo de mejora continua o de Deming. Dicho ciclo consiste, como ya sabemos, en Planificar – Hacer – Verificar - Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan – Do -Check - Act). Trasladado a las necesidades de un SGSI, el ciclo PDCA planteado por la ISO 27001 se dividiría en los siguientes pasos, cada uno de ellos ligado a una serie de acciones. (secc. Aspectos claves de un SGSI basado en la norma ISO 27001)

Tabla 2

Ciclo de Deming - PDCA

PLANIFICAR	Definir la política de seguridad. Establecer al alcance del SGSI. Realizar el análisis de riesgo. Seleccionar los controles. Definir competencias. Establecer un mapa de procesos. Definir autoridades y responsabilidades.
HACER	Implantar el plan de gestión de riesgos Implantar el SGSI. Implantar los controles.
CONTROLAR	Revisar internamente el SGSI. Realizar auditorías internas del SGSI. Poner en marcha indicadores y métricas. Hacer una revisión por parte de la Dirección.
ACTUAR	Adoptar acciones correctivas. Adoptar acciones de mejora.

Nota. ISO 27001. Aspectos claves y relación con las normas ISO 22301 e ISO/IEC 20000, por ESGINNOVA Group, 2019 (https://www.pmg-ssi.com/2019/08/iso-27001-aspectos-claves-y-relacion-con-las-normas-iso-22301-e-iso-iec-20000/).

2.4.2 ISO 27002 – 2013.

La norma ISO 27002-2013 Organización Internacional de Normalización (ISO, 2013): Proporciona un conjunto de pautas para controles de seguridad de la información comunes, así como instrucciones para su implementación. Se trata de la ciberseguridad y protección de datos y ha evolucionado desde su publicación inicial en 2005. En la actualidad, el contenido es más completo e integral y se centra en la gestión, la resiliencia, la protección y la defensa. Por otro lado, la ISO 27002 - 2013 incluye 14 dominios, 35 objetivos de control y 114 controles. El caso de investigación usará cuatro dominios, que son:

9. Control de Accesos

9.2.4 Gestión de información confidencial de autenticación de usuarios.

9.2.5 Revisión de los derechos de acceso de los usuarios.

9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.

9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información.

9.4.2 Procedimientos seguros de inicio de sesión.

9.4.3 Gestión de contraseñas de usuario.

9.4.4 Uso de herramientas de administración de sistemas.

9.4.5 Control de acceso al código fuente de los programas. (secc. A9 CONTROL DE ACCESO)

10. Cifrado

10.1 Controles criptográficos.

10.1.1 Política de uso de los controles criptográficos.

10.1.2 Gestión de claves. (secc. A10 CRIPTOGRAFIA)

17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

17.1 Continuidad de la seguridad de la información.

17.1.1 Planificación de la continuidad de la seguridad de la información.

17.1.2 Implantación de la continuidad de la seguridad de la información.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. (secc. A17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO)

18. Cumplimiento

18.1 Cumplimiento de los requisitos legales y contractuales.

18.1.1 Identificación de la legislación aplicable.

18.1.2 Derechos de propiedad intelectual (DPI).

18.1.3 Protección de los registros de la organización.

18.1.4 Protección de datos y privacidad de la información personal.

18.1.5 Regulación de los controles criptográficos. (secc. A18 CUMPLIMIENTO)

2.4.3 ISO 27017.

La norma ISO/IEC 27017 es una norma internacional que proporciona recomendaciones y requisitos para la implementación de medidas de seguridad y protección de la información en el contexto del Cloud Computing. Esta norma se centra en la protección de datos sensibles y proporciona recomendaciones para la implementación de medidas de seguridad y privacidad en entornos de Cloud computing. La norma ISO/IEC 27017 incluye una lista de requisitos para la implementación de medidas de seguridad y privacidad en el Cloud computing, incluyendo la protección de datos sensibles y la gestión de la seguridad de la información. Además, esta norma proporciona un marco de referencia para la evaluación y el monitoreo de la seguridad y la privacidad de la información en entornos de Cloud computing.

2.4.4 ISO 27033-4.

La norma ISO/IEC 27033-4 es una norma internacional que proporciona recomendaciones y requisitos para la implementación de medidas de seguridad de la red en entornos de red de computadoras. Esta norma se centra en la protección de datos sensibles y proporciona recomendaciones para la implementación de medidas de

seguridad de la red en diferentes entornos. La norma ISO/IEC 27033-4 incluye una lista de requisitos para la implementación de medidas de seguridad de la red, incluyendo la protección de datos sensibles y la gestión de la seguridad de la red. Además, esta norma proporciona un marco de referencia para la evaluación y el monitoreo de la seguridad de la red en diferentes entornos.

2.4.5 ISO 22301.

La norma ISO 22301 es un estándar internacional de gestión de la continuidad del negocio que establece los requisitos para la implementación y mantenimiento de un sistema de gestión de la continuidad del negocio (SGCN). Esta norma es publicada por la International Organization for Standardization (ISO) y es parte de la familia de normas ISO 22000.

La norma ISO 22301 establece un marco general para la gestión de la continuidad del negocio que incluye la identificación de los riesgos para la continuidad del negocio, la evaluación de estos riesgos y la implementación de medidas para mitigarlos. También incluye requisitos para la revisión y mejora continua del SGCN.

La norma ISO 22301 es ampliamente utilizada en todo el mundo para ayudar a las organizaciones a garantizar la continuidad del negocio en caso de desastres o eventos inesperados. Esta norma es aplicable a cualquier tipo de organización, independientemente de su tamaño o sector de actividad.

Para cumplir con la norma ISO 22301, las organizaciones deben implementar un SGCN y demostrar que cumplen con los requisitos establecidos en la norma a través de una auditoría independiente.

2.4.6 ISO 24761.

La norma ISO 24761 es una norma de la International Organization for Standardization (ISO) que establece los requisitos y las recomendaciones para la protección de datos personales en el contexto de la utilización de servicios de la información y de comunicación. Esta norma se aplica a cualquier organización que utilice servicios de la información y de comunicación y que maneje datos personales.

La norma ISO 24761 establece los requisitos para la protección de datos personales en el contexto de la utilización de servicios de la información y de comunicación, incluyendo la protección de datos personales durante el tratamiento, el almacenamiento y la transmisión de datos. También establece recomendaciones para garantizar la

confidencialidad, la integridad y la disponibilidad de los datos personales y para garantizar la privacidad de los usuarios de servicios de la información y de comunicación.

En resumen, la norma ISO 24761 es una norma que establece los requisitos y las recomendaciones para la protección de datos personales en el contexto de la utilización de servicios de la información y de comunicación. Esta norma es relevante para cualquier organización que utilice servicios de la información y de comunicación y que maneje datos personales.

2.4.7 ISO 19794-6.

La norma ISO/IEC 19794-6 es una norma internacional que establece los requisitos y las especificaciones para la captura, el almacenamiento y el intercambio de datos biométricos para el reconocimiento facial. Esta norma se centra en el uso de imágenes de cara para la identificación y autenticación de individuos y proporciona un marco para la representación de datos biométricos y para la evaluación de la calidad de las imágenes de la cara. La norma ISO/IEC 19794-6 forma parte de un conjunto más amplio de normas ISO/IEC 19794 que tratan de la representación de datos biométricos para diferentes características biométricas, como huellas dactilares, reconocimiento de voz y reconocimiento del iris.

2.4.8 NIST.

El National Institute of Standards and Technology (NIST) es una agencia del gobierno de los Estados Unidos, encargada de desarrollar estándares y tecnologías para mejorar la productividad y competitividad de la industria estadounidense. NIST también proporciona asesoramiento técnico y científico a otras agencias gubernamentales y al sector privado.

NIST es conocido por sus esfuerzos en áreas como la ciberseguridad, la tecnología de la información, la ingeniería y los sistemas de medición. Esto incluye la publicación de guías y recomendaciones para mejorar la seguridad cibernética, el desarrollo de estándares para la tecnología de la información y la investigación en avances tecnológicos y científicos.

NIST es una agencia independiente del gobierno de los Estados Unidos y está bajo la jurisdicción del Departamento de Comercio. Su sede principal se encuentra en Gaithersburg, Maryland, y cuenta con varias instalaciones en todo el país.

Figura 8

Marco de Ciberseguridad del NIST

Capability	Description
Identify	What processes and assets need protection?
Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
Respond	Develop techniques to contain the impacts of cybersecurity events
Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

Nota. Marco de Ciberseguridad del NIST. De "What is the NIST Cybersecurity Framework?". Por BALBIX. (https://www.balbix.com/insights/nist-cybersecurity-framework/)

2.4.8.1 NIST SP 800-76-2.

La Guía SP 800-76-2 de la NIST es una guía técnica que proporciona recomendaciones para la implementación y el uso de sistemas de identificación por biometría en redes de comunicación. Esta guía se centra en la identificación y autenticación de individuos a través del uso de características biométricas, como huellas dactilares, reconocimiento facial y reconocimiento de voz. La guía incluye recomendaciones para la implementación de sistemas de biometría en diferentes entornos y para asegurar la privacidad y la protección de datos sensibles. También proporciona información sobre la evaluación de la calidad de los sistemas de biometría y la gestión de la seguridad en sistemas biométricos.

2.4.8.2 NIST SP 800-145.

La Guía SP 800-145 de la NIST (National Institute of Standards and Technology) es una guía técnica que proporciona un marco para la evaluación y selección de sistemas de almacenamiento de datos de código abierto. Esta guía se centra en la selección de sistemas de almacenamiento de datos de código abierto para su uso en entornos gubernamentales, y proporciona información sobre cómo evaluar la calidad y la seguridad de estos sistemas. La guía incluye una lista de consideraciones clave para la selección de sistemas de almacenamiento de datos de código abierto y

proporciona recomendaciones para su implementación y uso. Además, la guía SP 800-145 incluye una lista de recursos adicionales para obtener más información sobre el uso de sistemas de almacenamiento de datos de código abierto en entornos gubernamentales.

2.4.8.3 NIST SP 800-207.

La Guía SP 800-207 de la NIST (National Institute of Standards and Technology) es una guía técnica que proporciona recomendaciones y consideraciones para la implementación y el uso de sistemas de hardware y software de protección de la privacidad. Esta guía se centra en la protección de datos sensibles y proporciona información sobre cómo diseñar y desplegar sistemas de hardware y software que cumplan con los requisitos de privacidad y seguridad. La guía incluye recomendaciones para la implementación de sistemas de hardware y software de protección de la privacidad en diferentes entornos, y proporciona información sobre la gestión de la seguridad y la privacidad en estos sistemas. Además, la guía SP 800-207 incluye una lista de recursos adicionales para obtener más información sobre la protección de la privacidad y la seguridad de datos sensibles.

3. Estado del arte

3.1 Introducción

El análisis del problema relacionado al control de acceso, autentificación de usuarios y vulnerabilidades para intrusiones llevó al desarrollo del presente trabajo de investigación que plantea un modelo de autenticación biométrica fisiológica o conductual para prevenir intrusiones en arquitecturas Cloud.

Se identificaron tres términos de búsqueda "Access Control", "Authentication Methods" y "Analysis of Vulnerability" con los que se formularon cuatro preguntas relacionadas al tema de investigación: ¿Qué métodos de autenticación pueden garantizar un control de acceso seguro para prevenir intrusiones en una arquitectura Cloud?, ¿qué herramientas de análisis de vulnerabilidades previenen el control de acceso para prevenir intrusiones en una arquitectura Cloud?, ¿qué métodos de autenticación pueden reducir las vulnerabilidades para prevenir intrusiones en una arquitectura Cloud? y ¿qué Framework de ciberseguridad se usa para mejorar el control de acceso de autenticación y análisis de vulnerabilidades en una arquitectura Cloud?; en base a estas cuatro preguntas se procedió a la búsqueda de información en los repositorios especializados de Scopus, IEEE Xplore y Web of Science aplicando las siguientes restricciones: Solo artículos publicados en journals salvo que sea un "conference paper" directamente relacionado al tema de estudio. Se excluyó información de años anteriores al 2018 que no han sido citados por otros autores y publicaciones que no aporten al tema de investigación.

La revisión de las lecturas, para identificar los artículos que mejor respondan a las preguntas planteadas, permitió al equipo de trabajo fortalecer las bases sobre las que se desarrollará la investigación y a determinar el rumbo de esta.

3.2 Revisión sistemática de la literatura

3.2.1 Búsqueda de palabras clave.

Selección de la búsqueda de las palabras clave que capten la idea central del proyecto de investigación.

Tabla 3

Búsqueda de palabras clave

Search Term	Web of Science	IEEE Xplore	Scopus
“Access Control”	235,981	107,000	62,148
“Security Servers”	7,291	25,609	117
“Authentication Methods”	9,783	10,132	3,533
“Data Privacy Policies”	3,878	3,729	64
“Analysis of Vulnerability”	48,952	8,468	344
“Hardening Computer”	2,145	2,517	4

Selección de las palabras claves que estén relacionados con el objeto de estudio y/o proyecto de investigación.

Tabla 4

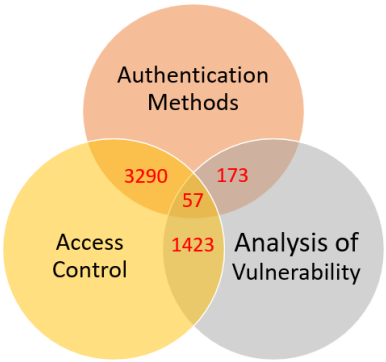
Selección de las palabras clave

Search Term	Web of Science	IEEE Xplore	Scopus	Total
Access Control” AND “Authentication Methods	574	2,444	272	3,290
“Access Control” AND “Analysis of Vulnerability”	918	501	4	1,423
“Authentication Methods” AND “Analysis of Vulnerability”	105	162	1	173
“Access Control” AND “Authentication Methods” AND “Analysis of Vulnerability	10	46	1	57

Con el diagrama de Venn con las **tres palabras clave más representativas** en la investigación y muestra la intersección entre ellas para tener un mejor análisis de la información.

Figura 9

Diagrama de Venn



3.2.2 Preguntas de investigación.

Después de seleccionar las palabras clave, se formulan cuatro preguntas de investigación (RQ) que nos van a permitir estructurar de manera correcta para poder resolver el problema de estudio.

Tabla 5

Preguntas de investigación

Search Term	Código	Preguntas
"Access Control" AND "Authentication Methods"	RQ1	¿Qué métodos de autenticación pueden garantizar un control de acceso seguro para prevenir intrusiones en una arquitectura Cloud?
"Access Control" AND "Analysis of Vulnerability"	RQ2	¿Qué herramientas de análisis de vulnerabilidades previenen el control de acceso para prevenir intrusiones en una arquitectura Cloud?
"Authentication Methods" AND "Analysis of Vulnerability"	RQ3	¿Qué métodos de autenticación pueden reducir las vulnerabilidades para prevenir intrusiones en una arquitectura Cloud?
"Access Control" AND "Authentication Methods" AND "Analysis of Vulnerability"	RQ4	¿Qué Framework de ciberseguridad se usa para mejorar el control de acceso de autenticación y análisis de vulnerabilidades en una arquitectura Cloud?

3.2.3 Estrategia y procesos de búsqueda.

Para la estrategia y procesos de búsqueda utilizaremos el framework PICOC y las consultas en Scopus, lo cual permitirá determinar el alcance de la investigación.

Pregunta 1:

Tabla 6

PICOC de la pregunta 1

	Research Question	**PICOC**		**Artículos encontrados SCOPUS**
"Access Control" AND "Authentication Methods"	RQ1: ¿Qué métodos de autenticación pueden garantizar un control de acceso seguro para prevenir intrusiones en una arquitectura Cloud?	P (POPULATION)	Users	32
		I (INTERVENTION)	Norms, Regulations, Standards	
		C (COMPARISON)		
		O (OUTCOME)	Protection, Privacy, Security, Intrusion	
		C (CONTEXT)	Technological infrastructure	

Consulta en Scopus:

("Access Control" AND ("Authentication Methods" OR "Infrastructure Technological") AND ("Norms" OR "Regulations" OR "Standards"))

Pregunta 2

Tabla 7

PICOC de la pregunta 2

	Research Question	PICOC		Artículos encontrados SCOPUS
“Access Control” AND “Analysis of Vulnerability”	RQ2: ¿Qué herramientas de análisis de vulnerabilidades previenen el control de acceso para prevenir intrusiones en una arquitectura Cloud?	P (POPULATION)	Users	239
		I (INTERVENTION)	Network, threats	
		C (COMPARISON)		
		O (OUTCOME)	Privacy, Information Protection, secure Access	
		C (CONTEXT)	Technological infrastructure	

Consulta en Scopus:

("Access Control" AND ("Analysis of Vulnerability" OR "Infrastructure Technological ") OR ("NETWORK" OR "threats") AND ("Secure Access"))

Pregunta 3

Tabla 8

PICOC de la pregunta 3

	Research Question	PICOC		Artículos encontrados SCOPUS
“Authentication Methods” AND “Analysis of Vulnerability”	RQ3:¿Qué métodos de autenticación pueden reducir las vulnerabilidades para prevenir intrusiones en una arquitectura Cloud?	P (POPULATION)	Users	51
		I (INTERVENTION)	QR Authentication, MFA, Biometrics, Digital Certificate	
		C (COMPARISON)		
		O (OUTCOME)	Protection, Privacy, Security, Intrusion	
		C (CONTEXT)	Technological infrastructure	

Consulta en Scopus:

("Authentication Methods" AND ("Vulnerabilities" OR "Infrastructure Technological") AND ("QR Authentication" OR "MFA" OR "Biometrics" OR "Digital Certificate"))

Pregunta 4

Tabla 9

PICOC de la pregunta 4

	Research Question	PICOC		Artículos encontrados SCOPUS
"Access Control" AND "Authentication Methods" AND "Analysis of Vulnerability"	RQ4: ¿Qué Framework de ciberseguridad se usa para mejorar el control de acceso de autenticación y análisis de vulnerabilidades en una arquitectura Cloud?	P (POPULATION)	Users	17
		I (INTERVENTION)		
		C (COMPARISON)	Techniques, frameworks, standards	
		O (OUTCOME)	Prevention, protection, privacy, authentication method, security	
		C (CONTEXT)	Technological infrastructure	

Consulta en Scopus:

("Access Control" AND "Authentication Methods" AND ("vulnerabilities" OR "Technological infrastructure" OR "Cloud"))

3.3 Metodología

Para seleccionar cada artículo científico relacionado al proyecto cuyo título es modelo de autenticación biométrica fisiológica o conductual para prevenir intrusiones en arquitecturas Cloud, la metodología que se aplicó se divide en tres fases:

- Planificación: Primero, se elaborará cada pregunta de la investigación usando un método para buscar e identificar cada artículo científico relacionado.
- Desarrollo: Segundo, fase concentrada en aplicar cada criterio para seleccionar y excluir cada estudio primario, se procederá a responder cada pregunta sobre la base de cada investigación encontrada.
- Resultados: En esta tercera fase, se presentará el análisis, el cual se basa en la matriz del conocimiento de esta investigación.

3.4 Planificación

3.4.1 Preguntas de investigación.

- Pregunta 1: ¿Qué métodos de autenticación pueden garantizar un control de acceso seguro para prevenir intrusiones en una arquitectura Cloud?
- Pregunta 2: ¿Qué herramientas de análisis de vulnerabilidades previenen el control de acceso para prevenir intrusiones en una arquitectura Cloud?
- Pregunta 3: ¿Qué métodos de autenticación pueden reducir las vulnerabilidades para prevenir intrusiones en una arquitectura Cloud?
- Pregunta 4: ¿Qué Framework de ciberseguridad se usa para mejorar el control de acceso de autenticación y análisis de vulnerabilidades en una arquitectura Cloud?

3.4.2 Bancos.

Los artículos científicos y académicos usados como base de la investigación fueron obtenidos de los siguientes repositorios especializados:

- Scopus
- Web of Science
- IEEE Xplore

3.4.3 Palabras claves.

A continuación, se muestran las palabras y los términos utilizados más representativos para la búsqueda de los artículos materia de investigación:

- “Access Control”
- “Authentication Methods”
- “Analysis of Vulnerability”

3.4.4 Periodo.

Las investigaciones que serán parte del estado del arte deben de cumplir con el periodo comprendido entre el 2018 y 2022.

3.4.5 Criterios de inclusión y exclusión.

Se aplicaron los criterios de selección y exclusión que se muestran en la tabla 10.

Tabla 10

Criterios de inclusión y exclusión

Criterios de Inclusión	Criterios de Exclusión
Artículos redactados en el idioma inglés relacionados al tema de investigación. Journals (Scopus, IEEE, Web of Science)	Artículos publicados antes del 2018.
Artículos y estudios más citados en ciberseguridad, control de acceso, vulnerabilidades, métodos de autentificación.	Publicaciones que no aporten temas sobre la investigación.
Artículos más citados.	Artículos que no usan referencias de validación.

3.5 Desarrollo

Los artículos seleccionados, de acuerdo con las preguntas formuladas, fueron 40, tal como se visualiza en la tabla 11.

Tabla 11

Artículos científicos seleccionados para el estudio

Question	Scopus	IEEE Xplore	Web of Science	TOTAL
RQ1	6	4	1	11
RQ2	4	3	2	9
RQ3	8	4	1	13
RQ4	3	4	0	7
TOTAL	21	15	4	40

Los 40 artículos científicos seleccionados fueron filtrados y agrupados en tres grupos de investigación, como se visualiza en la tabla 12. El grupo tiene cuatro artículos relacionados con el problema. El grupo siguiente o número dos tiene nueve artículos, los cuales se enfocan en diversas soluciones que hay para la cobertura del problema

presente. Por último, el grupo final tiene siete artículos que se orientan en técnicas que contribuyeron a solucionar el problema hallado.

Tabla 12

Artículos científicos seleccionados para el estudio

Grupo de investigación	Cuartil	Título	Autor	Año	Conference/Journal
Problema	Conferencia	Assessing frameworks for eliciting privacy & security requirements from laws and regulations	Olukoya Oluwafemi	2020	Artículo
	Q1	A review on performance, security and various biometric template protection schemes for biometric authentication systems	Arpita Sarkar & Binod K. Singh	2020	Artículo
	Conferencia	Intra-Cloud and Inter-Cloud Authentication	Walsh Kevin, Manferdelli John	2017	Artículo
	Q1	A Lightweight Attribute-Based Access Control Scheme for Intelligent Transportation System with Full Privacy Protection	Hui Tian, Xiang Li, Hanyu Quan, Chin-Chen Chang and Thar Baker	2021	Journal
Solución	Q1	User authentication on mobile devices: Approaches, threats and trends	Chen Wanga,d, Yan Wang b, Yingying Chena, Hongbo Liuc, Jian Liua	2020	Journal
	Q3	Emotion Recognition using Short-Term Multi-Physiological Signals	Tae-Koo Kang	2019	Artículo
	Q1	Zero Trust Architecture (ZTA): A Comprehensive Survey	Naeem Firdois Syed, Syed W. Shah, Arash Shaghaghi, Adnan Anwa, Zubair Baig and Robin Doss	2022	Artículo
	Conferencia	Evolving Authentication Design Consideration and BaaS Architecture for Internet of Biometric things	Pravin S. Jangid, Vinayak Ashok Bharad	2020	Conferencia
	Q2	Biometrics Using Electroencephalograms Stimulated by Personal Ultrasound and Multidimensional Nonlinear Features	Isao Nakanishi and Takehiro Maruoka	2019	Artículo
	Q1	Enhanced PKI authentication with trusted product at claimant	Asahiko Yamada, Tatsuro Ikeda	2017	Artículo

	Conferencia	A secure identity and Access Management framework in Cloud environment base on Dual-Factor Authentication	Faris Mudhhi Alruwaili, Ayman Mohamed Mostada, Osama Ouda	2021	Journal
	Conferencia	Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS	Diah Sulistyowati, Fitri Handayani, Yohan Suryanto	2020	Artículo
	Conferencia	Diverse Security Practices and Comparison on Key Stroke Dynamics	Praveen Kumar, Shagun Seth, Kanishka Bajaj, and Seema Rawat	2019	Conferencia
Técnica	Q2	Biometric ontology for semantic biometric-asa-service (BaaS) applications: a border security use case	Alper Kanak	2018	Artículo
	Q3	P2M-based security model: security enhancement using combined PUF and PRNG models for authenticating consumer electronic devices security use case	Paul Wortman , Wei Yan, John Chandy, Fatemeh Tehranipoor	2018	Artículo
	Q1	Computational workload in biometric identification systems: an overview	Pawel Drozdowski, Christian Rathgeb, Christoph Busch	2019	Artículo
	Q1	Finger vein biometrics: Taxonomy analysis, open challenges, future directions, and recommended solution for decentralised network architectures	A.H. Mohsin, A.A. Zaidan, B.B. Zaidan1, O.S. Albahri, Shamsul Arrieya Bin Ariffin, Ahmed Alemran, Odai Enaizan, Ali. H. Shareef, Ali Najm Jasim, N.S. Jalood, M.J. Baqer, A.H. Alamoodi, E.M. Almahdi, A.S. Albahri, M.A. Alsalem, K.I. Mohammed, H.A. Ameen, Salem Garfan	2020	Artículo
	Q1	A Three Layered Decentralized IoT Biometric	Kolhar, Manjura; Al-	2020	Artículo

		Architecture for City Lockdown during COVID-19 Outbreak	Turjman, Fadib; Alameen, Abdallaa; Abualhaj, Mosleh M.		
	Q1	A Novel Pairing-Free Lightweight Authentication Protocol for Mobile Cloud Computing Framework	Azeem Irshad , Shehzad Ashraf Chaudhry , Osama Ahmad Alomari, Khalid Yahya, and Neeraj Kumar	2022	Artículo
	Q1	Stable Hash Generation for Efficient Privacy-Preserving Face Identification	Dail ´e Osorio-Roig, Christian Rathgeb, Pawel Drozdowski, Christoph Busch	2021	Artículo

Cada artículo se resume a continuación respondiendo a cuatro preguntas de investigación que están relacionadas con el aporte del autor, el proceso utilizado para resolverlos, y sus principales resultados.

Pregunta 1: ¿Qué métodos de autenticación pueden garantizar un control de acceso seguro para prevenir intrusiones en una arquitectura Cloud?

Existen varios métodos de autenticación que pueden garantizar un control de acceso seguro para prevenir intrusiones. Algunos de los métodos más efectivos incluyen:

Autenticación de contraseña: Este es uno de los métodos de autenticación más comunes y se basa en que el usuario ingrese una contraseña secreta para acceder al sistema. Es importante que las contraseñas sean complejas y que los usuarios las cambien periódicamente para garantizar la seguridad.

Autenticación de dos factores (2FA): La autenticación de dos factores implica que los usuarios deben ofrecer dos tipos distintos de validación, como una contraseña junto con un código de seguridad enviado a su teléfono móvil o correo electrónico. Esta medida dificulta considerablemente que un intruso pueda acceder al sistema.

Autenticación biométrica: La autenticación biométrica utiliza características físicas o de comportamiento únicas, como huellas dactilares, reconocimiento facial o de voz, para identificar al usuario. Esto hace que sea muy difícil para alguien, que no es el usuario, acceder al sistema.

Autenticación de tarjeta inteligente: Las tarjetas inteligentes contienen un chip que almacena la información de autenticación y se pueden usar en lugar de contraseñas para acceder a un sistema. Esto hace que sea más difícil para los intrusos acceder al sistema.

Es importante tener en cuenta que ningún método de autenticación es completamente infalible, por lo que es importante implementar varias capas de seguridad para garantizar la seguridad del sistema.

Artículo N.° 1

Título:

User authentication on mobile devices: Approaches, threats and trends

Autores:

Chen Wang a, d, ∗, Yan Wang b, Yingying Chen a, Hongbo Liu c, Jian Liu a

Proceso:

- Revisión de literatura: El estudio revisa la literatura existente sobre autenticación de usuario en dispositivos móviles y describe los enfoques actuales utilizados en la industria y la academia.
- Análisis de amenazas: Se realiza un análisis de las amenazas y vulnerabilidades relacionadas con la autenticación de usuario en dispositivos móviles, incluyendo ataques de phishing, ataques de fuerza bruta, ataques de intercepción y ataques de robo de identidad.
- Descripción de enfoques de autenticación: El estudio describe los enfoques de autenticación de usuario en dispositivos móviles, incluyendo el uso de contraseñas, patrones de desbloqueo, autenticación biométrica y autenticación multifactor.
- Identificación de tendencias emergentes: Se identifican tendencias emergentes en la autenticación de usuario en dispositivos móviles, como el uso de la inteligencia artificial y el aprendizaje automático para mejorar la precisión de la autenticación, el uso de tecnologías de tokenización para proteger la información de autenticación y la creciente importancia de la privacidad de datos y la protección de datos biométricos.
- Evaluación de las soluciones existentes: El estudio evalúa algunas soluciones existentes de autenticación de usuario en dispositivos móviles, como Apple Face ID, Google Smart Lock y Microsoft.

Resultado:

En general, el paper destaca la necesidad de soluciones de autenticación más seguras en dispositivos móviles, describe los enfoques actuales y emergentes utilizados en la industria y la academia. También se destacan las amenazas y desafíos asociados con la autenticación de usuario en dispositivos móviles y se discuten las tendencias emergentes en esta área. Los

resultados del estudio pueden ser útiles para los desarrolladores de aplicaciones móviles y los usuarios finales que deseen mejorar la seguridad de la autenticación en sus dispositivos móviles.

Conclusión:

Es que la autenticación de usuario en dispositivos móviles es un desafío importante debido al aumento de la popularidad de estos dispositivos y la necesidad de soluciones de autenticación más seguras. El uso de contraseñas y patrones de desbloqueo sigue siendo común, pero estas formas de autenticación son vulnerables a diversos ataques. La autenticación biométrica se está volviendo cada vez más popular, pero también hay preocupaciones sobre la privacidad y seguridad de los datos biométricos. La autenticación multifactor es una solución más segura y se está volviendo más común en dispositivos móviles. El paper también destaca la importancia de la privacidad y seguridad de los datos biométricos y discute las tecnologías emergentes que se están utilizando para mejorar la precisión y seguridad de la autenticación de usuario en dispositivos móviles. En general, se concluye que hay una necesidad continua de soluciones de autenticación más seguras en dispositivos móviles y que los desarrolladores de aplicaciones móviles y los usuarios finales deben considerar una variedad de enfoques de autenticación para lograr un equilibrio entre la seguridad y la comodidad.

Artículo N.° 2

Título:

Diverse Security Practices and Comparison on Key Stroke Dynamics

Autores:

Praveen Kumar1, Shagun Seth2, Kanishka Bajaj3 and Seema Rawat4 1,2,3,4Amity University Uttar Pradesh, Noida

Proceso:

- Introducción de la dinámica de pulsación de teclas como método de autenticación biométrica.
- Descripción de los diferentes tipos de autenticación biométrica, incluyendo la dinámica de pulsación de teclas.

- Análisis de las prácticas de seguridad en diferentes sistemas de autenticación biométrica basados en dinámica de pulsación de teclas.
- Descripción de los conjuntos de datos utilizados en la comparación de diferentes sistemas de autenticación biométrica basados en dinámica de pulsación de teclas.
- Presentación de los resultados de la comparación de diferentes sistemas de autenticación biométrica basados en dinámica de pulsación de teclas.
- Discusión de los resultados y conclusiones sobre la eficacia de los diferentes sistemas de autenticación biométrica basados en dinámica de pulsación de teclas.

Resultado:

- Se encontró que la autenticación basada en la dinámica de pulsación de teclas es efectiva y precisa en la mayoría de los sistemas de autenticación estudiados.
- Se identificaron diferentes prácticas de seguridad en los sistemas de autenticación basados en dinámica de pulsación de teclas, incluyendo el uso de características dinámicas y estáticas, y la combinación de diferentes tipos de características.
- Se encontró que el tamaño del conjunto de datos utilizado para entrenar el modelo de autenticación es un factor crítico para la precisión de la autenticación.
- Se encontró que el uso de técnicas de preprocesamiento, como la normalización de los datos, puede mejorar la precisión de la autenticación.
- Se encontró que la precisión de la autenticación puede disminuir en ciertas situaciones, como cuando el usuario está bajo estrés o fatiga.

Conclusión:

La conclusión del paper "Diverse Security Practices and Comparison on Key Stroke Dynamics" es que la dinámica de pulsación de teclas es un método efectivo de autenticación biométrica que puede ser utilizado en una variedad de sistemas de autenticación. Además, existen diferentes prácticas de seguridad que pueden mejorar la precisión de la autenticación, como el uso de características dinámicas y estáticas, y la combinación de diferentes tipos de características. El tamaño del conjunto de datos utilizado para entrenar el modelo de autenticación y las técnicas de preprocesamiento también son factores importantes que afectan la precisión de la autenticación basada en la

dinámica de pulsación de teclas. En general, la dinámica de pulsación de teclas es una opción viable para la autenticación biométrica y puede ser utilizada como una capa adicional de seguridad en sistemas de autenticación.

Pregunta 2: ¿Qué herramientas de análisis de vulnerabilidades previenen el control de acceso para prevenir intrusiones en una arquitectura Cloud?

Existen diversas herramientas de análisis de vulnerabilidades que pueden ayudar a prevenir el control de acceso para prevenir intrusiones en una arquitectura Cloud. Algunas de ellas son las siguientes:

Escáneres de vulnerabilidades: Estas herramientas escanean los sistemas y aplicaciones en busca de vulnerabilidades conocidas y las reportan para que puedan ser corregidas. Algunos ejemplos de escáneres de vulnerabilidades son Nessus, OpenVAS, Qualys y Nexpose.

Penetration testing (pruebas de penetración): Esta es una técnica de prueba que simula un ataque real para evaluar la seguridad de los sistemas y aplicaciones. Los pentesters buscan vulnerabilidades explotables y proporcionan recomendaciones para remediarlas. Ejemplos de herramientas de prueba de penetración incluyen Metasploit, Nmap y Wireshark.

Gestión de identidades y accesos (IAM): Estas herramientas administran los permisos de los usuarios en los sistemas y aplicaciones, lo que ayuda a prevenir el acceso no autorizado. Las herramientas IAM permiten a los administradores definir roles, políticas y permisos de acceso para los usuarios, lo que limita el acceso a los recursos del sistema. Ejemplos de herramientas IAM incluyen Google Cloud, Microsoft Active Directory, Okta y OneLogin.

Sistemas de detección de intrusos (IDS) y prevención de intrusos (IPS): Estas herramientas detectan y previenen intrusiones en los sistemas y aplicaciones. Los IDS monitorean la red en busca de actividades sospechosas, mientras que los IPS bloquean el tráfico que se considera malicioso. Ejemplos de herramientas IDS/IPS incluyen Snort, Suricata y Bro.

<u>Análisis de logs:</u> Estas herramientas analizan los registros de los sistemas y aplicaciones en busca de actividades sospechosas que puedan indicar una intrusión. Ejemplos de herramientas de análisis de logs incluyen Splunk, ELK Stack y Graylog.

Es importante destacar que estas herramientas deben ser utilizadas junto con buenas prácticas de seguridad, como la implementación de políticas de seguridad sólidas, la educación del usuario final, la actualización y parcheo de los sistemas y aplicaciones para garantizar una seguridad completa.

Artículo N.° 1

Título:

A Secure Identity and Access Management Framework in Cloud Environment Based on Dual-Factor Authentication

Autores:

Faris Mudhhi Alruwaili, Ayman Mohamed Mostafa and Osama Ouda

Proceso:

- Propone un marco de trabajo para la gestión de identidad y acceso seguro en entornos de nube basado en la autenticación de doble factor. El marco de trabajo propuesto consta de los siguientes procesos:
- Registro de usuario: El primer paso del proceso es el registro de usuario. En este paso, se solicita al usuario que proporcione su información de identidad y credenciales para crear una cuenta de usuario en el sistema.
- Autenticación de primer factor: Una vez que se ha registrado un usuario, se realiza la autenticación de primer factor, donde se verifica la identidad del usuario mediante el uso de credenciales, como un nombre de usuario y una contraseña.
- Autenticación de segundo factor: Después de la autenticación de primer factor, se realiza la autenticación de segundo factor, que se basa en algo que el usuario posee, como un token de seguridad o un teléfono móvil. Este segundo factor de autenticación agrega una capa adicional de seguridad al proceso de autenticación.
- Autorización de acceso: Una vez que se ha autenticado al usuario, el siguiente paso es la autorización de acceso. En este paso, se verifica que el usuario tenga los permisos necesarios para acceder a los recursos de la nube que desea.

- Auditoría de seguridad: Por último, el marco de trabajo propuesto incluye un proceso de auditoría de seguridad para garantizar que se sigan las mejores prácticas de seguridad y que se detecten y resuelvan las posibles vulnerabilidades en el sistema.

Resultado:

- Incluye una evaluación de la efectividad del marco de trabajo propuesto mediante un estudio de caso. En el estudio de caso, se implementó el marco de trabajo propuesto en una empresa de servicios financieros para proteger los datos de los clientes en la nube. La implementación del marco de trabajo propuesto resultó en una mejora significativa en la seguridad y la protección de los datos de los clientes.
- En particular, se observó que el uso de la autenticación de doble factor redujo el riesgo de acceso no autorizado a la nube, mientras que el proceso de auditoría de seguridad ayudó a detectar y solucionar posibles vulnerabilidades en el sistema. En general, el marco de trabajo propuesto se consideró efectivo para proteger los datos sensibles en la nube y para garantizar la seguridad de la información.

Conclusión:

El marco de trabajo propuesto ofrece una solución efectiva para la gestión de identidad y acceso seguro en entornos de nube y puede ser utilizado por empresas y organizaciones que deseen mejorar la seguridad de sus datos en la nube.

Artículo N.° 2

Titulo:

Zero Trust Architecture (ZTA): A Comprehensive Survey

Autores:

Naeem Firdous Syed, Syed w. Shah, Arash Shaghaghi, Adnan Anwar, Zubair Baig, and Robin Doss

Proceso:

Los procesos que se describen en el documento son los siguientes:

- Evaluación continua de la confianza: La evaluación continua de la confianza es un

proceso clave de la arquitectura Zero Trust. En este proceso, se realiza una evaluación constante de la confianza de los usuarios, dispositivos y aplicaciones antes de conceder el acceso a los recursos de la red.

- Identidad y autenticación: La identidad y autenticación son procesos críticos en la arquitectura Zero Trust. En este proceso, se autentica la identidad del usuario y se verifica que tenga los permisos necesarios para acceder a los recursos de la red.
- Autorización y acceso: La autorización y el acceso son procesos que determinan los recursos y servicios a los que un usuario o dispositivo pueden acceder. En la arquitectura Zero Trust, estos procesos se basan en la evaluación continua de la confianza y la autenticación de la identidad del usuario.
- Segmentación y microsegmentación: La segmentación y microsegmentación son procesos que permiten dividir la red en segmentos más pequeños y controlar el acceso a los recursos y servicios dentro de cada segmento. Esto reduce el riesgo de movimientos laterales dentro de la red en caso de que un dispositivo o usuario sea comprometido.
- Políticas de seguridad y automatización: La implementación de políticas de seguridad y automatización son procesos que permiten definir y aplicar reglas y políticas de seguridad para garantizar la protección de los datos y recursos de la red. La automatización ayuda a simplificar la gestión y aplicación de estas políticas.

Resultado:

Los resultados principales incluyen lo siguiente:

- La arquitectura Zero Trust se ha convertido en un enfoque cada vez más popular para proteger los sistemas de información y los datos de las organizaciones. Esta arquitectura se basa en la premisa de que no se debe confiar en ningún usuario, dispositivo o servicio dentro de la red, y se deben aplicar medidas de seguridad en cada nivel para minimizar el riesgo de vulnerabilidades y ataques.
- La implementación de la arquitectura Zero Trust requiere una planificación y una estrategia cuidadosas, y se debe realizar un análisis de riesgos para determinar las áreas más vulnerables de la red. Los procesos clave de la arquitectura Zero Trust incluyen la evaluación continua de la confianza, la identidad y autenticación, la

autorización y acceso, la segmentación y microsegmentación, y las políticas de seguridad y automatización.

- Las soluciones de seguridad de Zero Trust están evolucionando constantemente para satisfacer las demandas cambiantes de las empresas y los avances en tecnología. Además, la implementación de una arquitectura Zero Trust puede mejorar la visibilidad y el control de la seguridad de la red, y puede proporcionar una mayor protección contra amenazas internas y externas.

Sin embargo, la implementación de una arquitectura Zero Trust puede ser un desafío para las organizaciones, especialmente las más grandes y complejas. La implementación de políticas de seguridad y la segmentación de la red pueden ser complicadas, y puede ser difícil equilibrar la seguridad con la accesibilidad y la usabilidad de los recursos de la red.

Conclusión:

Es un enfoque valioso, efectivo para mejorar la seguridad de la red, proteger los sistemas de información y los datos de las organizaciones. El documento destaca que la implementación de una arquitectura Zero Trust requiere una planificación, una estrategia cuidadosa, que los procesos clave incluyen la evaluación continua de la confianza, la identidad y autenticación, la autorización y acceso, la segmentación y microsegmentación, y las políticas de seguridad y automatización.

Pregunta 3: ¿Qué métodos de autenticación pueden reducir las vulnerabilidades para prevenir intrusiones en una arquitectura Cloud?

Existen varios métodos de autenticación que pueden reducir las vulnerabilidades para prevenir intrusiones en una arquitectura Cloud. Algunos de ellos son los siguientes:

Autenticación multifactorial: Este método utiliza dos o más factores de autenticación para verificar la identidad del usuario, como una contraseña y un código de verificación enviado al dispositivo móvil del usuario. Al agregar una capa adicional de autenticación, se reduce la probabilidad de que un atacante pueda acceder al sistema con credenciales robadas.

Autenticación basada en certificados: Este método utiliza certificados digitales para verificar la identidad del usuario. Un certificado digital es un archivo electrónico que se utiliza para garantizar la identidad del usuario. Los certificados digitales se emiten a los usuarios por una autoridad de certificación confiable y pueden ser utilizados en combinación con una contraseña.

Autenticación biométrica: Este método utiliza características únicas del cuerpo humano para autenticar la identidad del usuario, como huellas dactilares, reconocimiento facial, iris, voz, entre otros. Las características biométricas son difíciles de falsificar, lo que reduce la probabilidad de que un atacante pueda acceder al sistema con credenciales robadas.

Autenticación de dispositivo: Este método utiliza características del dispositivo del usuario, como la dirección MAC, para autenticar la identidad del usuario. Al restringir el acceso a un dispositivo en particular, se reduce la probabilidad de que un atacante pueda acceder al sistema con credenciales robadas.

Autenticación de contraseña única (OTP): Este método utiliza una contraseña de un solo uso generada por un dispositivo de seguridad, como un token de autenticación o una aplicación móvil, para autenticar la identidad del usuario. Al utilizar una contraseña que solo se puede utilizar una vez, se reduce la probabilidad de que un atacante pueda acceder al sistema con credenciales robadas.

Artículo N.° 1

Titulo:

Biometric ontology for semantic biometric-asa-service (BaaS) applications: a border security use case

Autores:

Alper Kanak

Proceso:

Los procesos descritos en el artículo son los siguientes:

- Análisis de requisitos: se realiza un análisis de los requisitos de la aplicación de BaaS en el contexto de seguridad fronteriza.
- Desarrollo de la ontología biométrica: se desarrolla una ontología biométrica semántica que cubre los conceptos relevantes en el contexto de seguridad fronteriza.

- Desarrollo del sistema BaaS: se desarrolla un sistema de BaaS que utiliza la ontología biométrica para proporcionar servicios de biometría semántica.
- Evaluación del sistema BaaS: se evalúa el sistema de BaaS utilizando un conjunto de datos de biometría y se comparan los resultados con los obtenidos por un sistema de biometría convencional.
- Validación de la ontología biométrica: se valida la ontología biométrica utilizando el sistema de BaaS y se comprueba que es capaz de proporcionar servicios de biometría semántica de manera efectiva en el contexto de seguridad fronteriza.

Resultado:

- Desarrollo de la ontología biométrica: se desarrolló una ontología biométrica semántica que cubre los conceptos relevantes en el contexto de seguridad fronteriza. La ontología se basa en el estándar OWL (Web Ontology Language) y es capaz de representar la información semántica de manera clara y estructurada.
- Desarrollo del sistema BaaS: se desarrolló un sistema de BaaS que utiliza la ontología biométrica para proporcionar servicios de biometría semántica. El sistema permite la integración de diferentes tecnologías biométricas y su uso para diferentes fines en el contexto de seguridad.
- Evaluación del sistema BaaS: se evaluó el sistema de BaaS utilizando un conjunto de datos de biometría y se compararon los resultados con los obtenidos por un sistema de biometría convencional. Los resultados mostraron que el sistema de BaaS es capaz de proporcionar servicios de biometría semántica de manera efectiva y superar en rendimiento al sistema de biometría convencional.
- Validación de la ontología biométrica: se validó la ontología biométrica utilizando el sistema de BaaS y se comprobó que es capaz de proporcionar servicios de biometría semántica de manera efectiva en el contexto de seguridad. Además, se comprobó que la ontología es fácilmente extensible y puede ser utilizada en diferentes aplicaciones de biometría.

Conclusión:

El sistema de BaaS desarrollado proporciona servicios de biometría semántica que son más

precisos y rápidos que los sistemas de biometría convencionales, lo que permite mejorar la seguridad y la eficiencia en la gestión.

Artículo N.° 2

Título:

Evolving Authentication Design Consideration and BaaS Architecture for Internet of Biometric things

Autores:

Pravin S. Jangid y Vinayak Ashok Bharadi

Proceso:

Los procesos descritos en el paper son los siguientes:

- Revisión de la literatura existente sobre autenticación basada en biometría y los desafíos de seguridad en el IoT.
- Propuesta de una arquitectura de servicios de autenticación basada en biometría, denominada "Biometric-as-a-Service" (BaaS), para el IoT. La arquitectura propuesta incluye componentes como un servidor de autenticación, una plataforma de BaaS y un cliente de autenticación.
- Discusión de las consideraciones de diseño para la autenticación basada en biometría en el IoT, como la selección de la tecnología biométrica adecuada, la protección de la privacidad del usuario y la seguridad de los datos.
- Descripción de la implementación de la arquitectura de BaaS propuesta utilizando tecnologías de contenerización y orquestación.
- Evaluación de la arquitectura de BaaS propuesta y discusión de los resultados, incluyendo la escalabilidad, el rendimiento y la seguridad.

Resultado:

- Propuesta de una arquitectura de servicios de autenticación basada en biometría, denominada "Biometric-as-a-Service" (BaaS), para el IoT. La arquitectura propuesta puede ser utilizada para autenticar usuarios en diferentes dispositivos IoT,

como wearables y sensores.

- Descripción de las consideraciones de diseño para la autenticación basada en biometría en el IoT, como la selección de la tecnología biométrica adecuada, la protección de la privacidad del usuario y la seguridad de los datos.
- Implementación de la arquitectura de BaaS propuesta utilizando tecnologías de contenerización y orquestación, lo que permite una mayor escalabilidad y flexibilidad.
- Evaluación de la arquitectura de BaaS propuesta y discusión de los resultados. Los resultados muestran que la arquitectura propuesta es escalable, tiene un buen rendimiento y es segura.

Conclusión:

El artículo discute las consideraciones de diseño para la autenticación basada en biometría en el IoT, como la selección de la tecnología biométrica adecuada, la protección de la privacidad del usuario y la seguridad de los datos. Además, se propone una arquitectura de BaaS para la autenticación basada en biometría en el IoT, que incluye un servidor de autenticación, una plataforma de BaaS y un cliente de autenticación.

La implementación de la arquitectura propuesta utilizando tecnologías de contenerización y orquestación permite una mayor escalabilidad y flexibilidad en la implementación de la solución. Los resultados de la evaluación de la arquitectura de BaaS propuesta muestran que es escalable, tiene un buen rendimiento y es segura.

Pregunta 4: ¿Qué Framework de ciberseguridad se usa para mejorar el control de acceso de autenticación y análisis de vulnerabilidades en una arquitectura Cloud?

Existen varios Frameworks de ciberseguridad que se utilizan para mejorar el control de acceso de autenticación y análisis de vulnerabilidades en arquitecturas Cloud. Algunos de ellos son:

CIS Controls: Los CIS Controls (anteriormente conocidos como SANS Top 20) son un conjunto de controles de seguridad que se centran en la prevención y detección de ataques

cibernéticos. Los controles se dividen en tres niveles: Básico, Intermedio y Avanzado, y están diseñados para ser implementados en función del tamaño y la complejidad de la organización.

NIST Cybersecurity Framework: El marco de ciberseguridad del NIST es un conjunto de estándares, directrices y mejores prácticas que se utilizan para mejorar la ciberseguridad en organizaciones de todos los tamaños y sectores. El marco consta de cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperar.

ISO/IEC 27001: La norma ISO/IEC 27001 define los requisitos para un sistema de gestión de seguridad de la información (SGSI). Esta estándar define un conjunto de controles para la gestión de la seguridad de la información, donde se incluye la autenticación y el análisis de vulnerabilidades.

Estos Frameworks y modelos de ciberseguridad proporcionan una guía para implementar controles de seguridad efectivos que pueden ayudar a mejorar el control de acceso de autenticación y análisis de vulnerabilidades en una arquitectura Cloud. Es importante tener en cuenta que estos Frameworks no son una solución única para todas las organizaciones y deben adaptarse a las necesidades específicas de cada organización.

Artículo N.° 1

Titulo:

Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS

Autores:

Diah Sulistyowati, Fitri Handayani y Yohan Suryanto

Proceso:

- Revisión de los marcos de referencia de seguridad de la información NIST CSF, COBIT, ISO/IEC 27002 y PCI DSS. Se describen las fortalezas y debilidades de cada marco y se destacan las áreas de solapamiento y complementariedad entre ellos.
- Definición de una metodología de evaluación de madurez de ciberseguridad. La metodología se basa en la combinación de los marcos de referencia NIST CSF, COBIT, ISO/IEC 27002 y PCI DSS. Se describen los pasos necesarios para llevar a

cabo la evaluación de madurez, desde la planificación hasta la implementación y seguimiento.

- Descripción de los criterios de evaluación de madurez de ciberseguridad, basados en los marcos de referencia mencionados anteriormente. Los criterios se agrupan en seis categorías: gobierno de la seguridad de la información, gestión de riesgos, cumplimiento, seguridad operativa, seguridad técnica y continuidad del negocio.
- Implementación de la metodología de evaluación de madurez de ciberseguridad en un caso de estudio en una organización del sector financiero. Se describen los resultados de la evaluación y se destacan las áreas de mejora.
- Discusión de las conclusiones y recomendaciones para futuras investigaciones. Se discuten las limitaciones de la metodología propuesta y se sugieren posibles mejoras.

Resultado:

- Se proporciona una visión general de los marcos de referencia de seguridad de la información NIST CSF, COBIT, ISO/IEC 27002 y PCI DSS, incluyendo sus fortalezas y debilidades.
- Se desarrolla una metodología de evaluación de madurez de ciberseguridad basada en la combinación de los marcos de referencia mencionados anteriormente.
- Se describen los criterios de evaluación de madurez de ciberseguridad, organizados en seis categorías: gobierno de la seguridad de la información, gestión de riesgos, cumplimiento, seguridad operativa, seguridad técnica y continuidad del negocio.
- Se lleva a cabo un caso de estudio en una organización del sector financiero para demostrar la aplicabilidad de la metodología propuesta. Los resultados de la evaluación muestran las áreas de mejora y destacan la importancia de una evaluación integral de la madurez de la ciberseguridad.
- Se discuten las limitaciones de la metodología propuesta y se proponen posibles mejoras para futuras investigaciones.

Conclusión:

Es que la metodología de evaluación de madurez de ciberseguridad propuesta puede ser útil

para ayudar a las organizaciones a evaluar su nivel de madurez de ciberseguridad y a identificar áreas de mejora. La combinación de los marcos de referencia NIST CSF, COBIT, ISO/IEC 27002 y PCI DSS permite una evaluación integral de la madurez de la ciberseguridad en una organización.

Además, se destaca la importancia de la evaluación de la madurez de la ciberseguridad en la actualidad, ya que las organizaciones están cada vez más expuestas a ciberataques y necesitan estar preparadas para prevenirlos o mitigar sus efectos.

Se mencionan también algunas limitaciones de la metodología propuesta, como la necesidad de adaptarla a las características específicas de cada organización y de mantenerla actualizada en función de los cambios en los marcos de referencia de seguridad de la información.

En general, se concluye que la metodología propuesta puede ser una herramienta valiosa para las organizaciones que buscan mejorar su ciberseguridad y protegerse de los riesgos asociados a los ciberataques.

3.6 Resultados

✓ **Aspectos cubiertos**

De acuerdo con la investigación realizada de los cuarenta papers, se agruparon en tipo de contribución, tal como se muestra en la tabla 13.

Tabla 13

Investigaciones por tipo de contribución

TIPO DE CONTRIBUCIÓN	REFERENCIAS	TOTAL
SOFTWARE	[PAPER12], [PAPER19], [PAPER21], [PAPER24], [PAPER31, [PAPER32, [PAPER04], [PAPER5]	**8**
ALGORITMO	[PAPER38], [PAPER22], [PAPER23], [PAPER30], [PAPER2]	**5**
HERRAMIENTA	[PAPER17]	**1**
ARQUITECTURA	[PAPER16], [PAPER25], [PAPER33]	**3**
PROCEDIMIENTO	[PAPER1]	**1**
MODELO	[PAPER13], [PAPER14], [PAPER20], [PAPER34], [PAPER36], [PAPER28]	**6**
MÉTODO	[PAPER15], [PAPER18], [PAPER35], [PAPER37], [PAPER40], [PAPER26], [PAPER27], [PAPER29], [PAPER8]	**9**
BUENAS PRÁCTICAS	[PAPER39], [PAPER3]	**2**
ESTÁNDAR	[PAPER6]	**1**
REGULACIÓN	[PAPER7], [PAPER11]	**2**
CASO DE ESTUDIO	[PAPER10]	**1**
FRAMEWORK	[PAPER9]	**1**

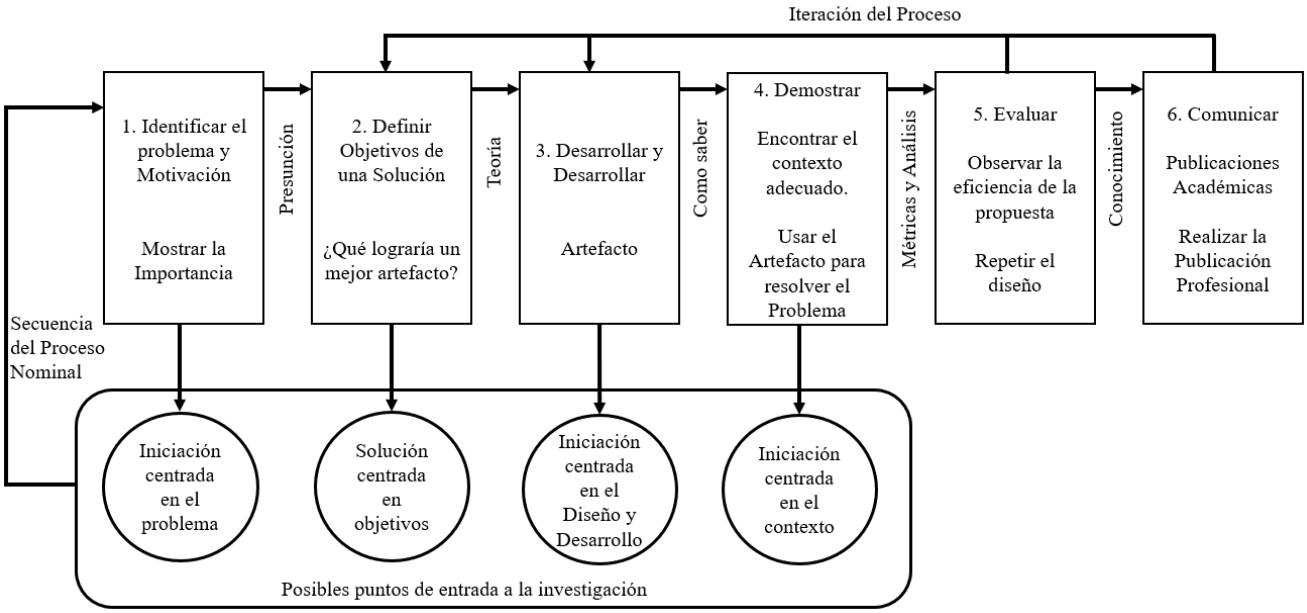
4. Proceso para el desarrollo del artefacto

4.1 Metodología de la Investigación

Es en base a Design Science Research Methodology For Information Systems, en el que se observa el proceso de la investigación.

Figura 10

Diagrama de la metodología Design Science Research Methodology For Information Systems



Nota. Diagrama de la metodología. De "Design Science Research Methodology for Information Systems". Por "Chatterjee et al., 2007".

4.1.1 Tipo y diseño de la investigación.

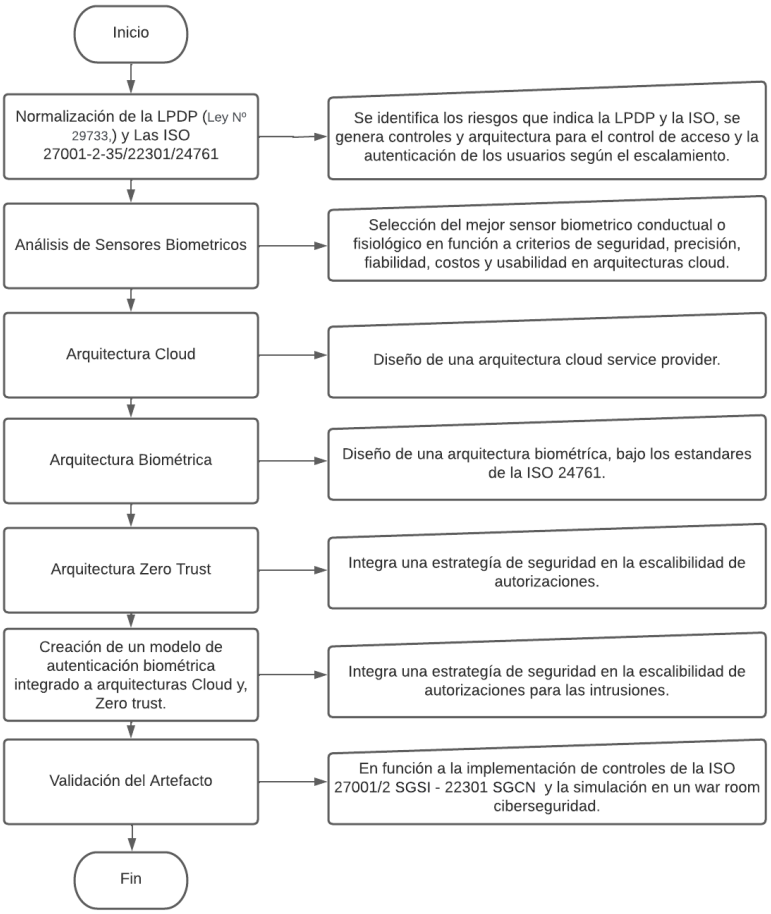
De acuerdo con las características de la investigación será de tipo descriptivo con un diseño no experimental asociado a un caso de estudio como método de validación.

4.1.2 Hoja de ruta para el desarrollo del artefacto.

El proceso del artefacto se define a través de los siguientes pasos.

Figura 11

Diagrama Diseño de la construcción del artefacto

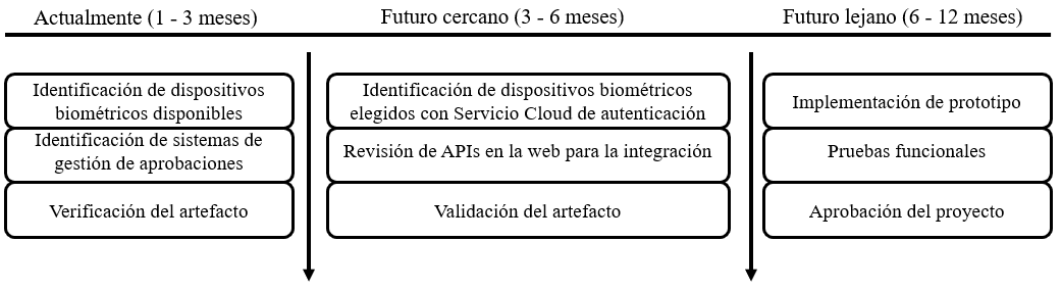


4.1.3 Plan de trabajo.

Se segmenta en función del desarrollo de la investigación.

Figura 12

Plan de trabajo

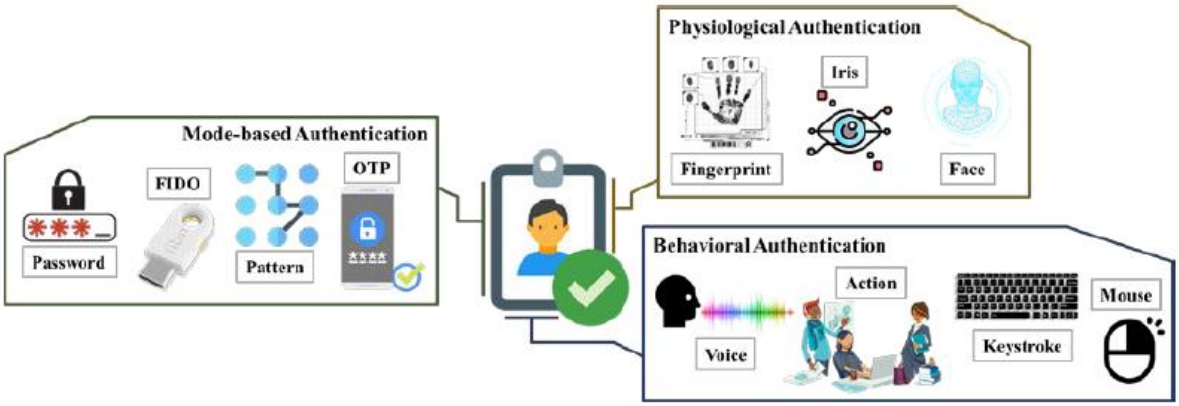


4.2 Análisis de la solución

Se pueden clasificar como métodos de autenticación de usuarios los siguientes: basado en modo, fisiológico y conductual.

Figura 13

Categorías de autenticación de usuarios



Nota. De Behavioral Analysis Zero-Trust Architecture Relying on Adaptive Multifactor and Threat Determination por Chit-Jie Chew et al, 2023.

El método basado en modos es la prueba de identidad más adoptada en sistemas arbitrarios, que incorpora contraseña, FIDO, patrón y contraseña de un solo uso (OTP). Aunque ofrece comodidad a los usuarios, el proceso de autenticación está potencialmente bajo riesgo de ataques de tablas arcoíris, filtración de contraseñas de vulnerabilidad del dispositivo y malware de interceptación de OTP.

La fisiología y el comportamiento son las características biológicas más representativas de una persona, lo que mejora significativamente la seguridad integral de la autenticación de identidad.

Para nuestra investigación, nos centraremos en el análisis de sensores biométricos fisiológicos y conductuales que permitan prevenir intrusiones en arquitecturas Cloud; basados en las buenas prácticas de la ISO 27001 y la LPDP.

4.2.1 Análisis de sensores biométricos para prevenir intrusiones, en conformidad con la Ley de Protección de Datos Personales (LPDP N.° 29733) y la Organización Internacional de Normalización (ISO 27001) en arquitecturas Cloud.

Los sensores biométricos, tanto fisiológicos como conductuales, son dispositivos o sistemas que se utilizan para medir y capturar características únicas y distintivas de una persona, que se utilizan en aplicaciones de identificación y autenticación.

Sensores Biométricos Fisiológicos:

Huella dactilar: Los sensores de huella dactilar capturan imágenes de las crestas y surcos de la piel de los dedos. Las huellas dactilares son únicas para cada individuo debido a la configuración específica de estos patrones.

Reconocimiento facial: Estos sensores utilizan cámaras para capturar y analizar características faciales, como la distancia entre los ojos, la forma de la nariz y la disposición de las cejas. Se basa en características físicas únicas del rostro de una persona.

Escáner de retina: Los escáneres de retina utilizan luz infrarroja para capturar imágenes de los vasos sanguíneos en la retina del ojo. La retina es altamente única y estable con el tiempo.

Escáner de iris: Los escáneres de iris capturan imágenes del patrón del iris, la parte coloreada del ojo. El patrón del iris es altamente distintivo y estable, lo que lo hace adecuado para la autenticación.

Reconocimiento de voz: Los sensores de reconocimiento de voz analizan características de la voz, como tono, patrones de habla y otros atributos vocales únicos para autenticar a una persona.

Sensores Biométricos Conductuales:

Dinámica de escritura: Los sensores de dinámica de escritura registran cómo una persona escribe, incluyendo la velocidad, la presión y el estilo de escritura. Estos patrones son específicos de cada individuo.

Reconocimiento de gestos: Utilizando cámaras y sensores de movimiento, el reconocimiento de gestos identifica patrones de gestos y movimientos únicos de una persona, como los gestos de la mano o el comportamiento del usuario en dispositivos táctiles.

Firma dinámica: Los sensores de firma dinámica capturan el comportamiento de firma de una persona, incluyendo la velocidad, la presión y la forma de la firma. Estos patrones son distintivos y se utilizan para verificar la identidad.

Análisis de pulsos y ritmo cardíaco: Los sensores de ritmo cardíaco y pulso miden las características únicas del ritmo cardíaco y el pulso, que pueden ser utilizados para la autenticación y la identificación.

Reconocimiento de patrones de tecleo: Los sensores de reconocimiento de patrones de tecleo analizan la forma en que una persona escribe en un teclado, incluyendo la velocidad, el patrón de pulsación de teclas y el estilo de escritura al escribir.

El análisis de la selección de los sensores para la biometría conductual o fisiológica se llevó a cabo considerando los indicadores de seguridad, precisión, eficacia, usabilidad, privacidad y costo.

4.2.2 Análisis de los sensores biométricos a través de métricas.

FAR (False Acceptance Rate): este parámetro se determina a partir del porcentaje de cuántas veces los sistemas de autenticación permitieron a un impostor como usuario legítimo. Esto se conoce como la tasa de coincidencia falsa (FMR) que se estima mediante la fórmula que sé que se indica a continuación.

FRR (False Rejection Rate): Este parámetro se describe a partir del porcentaje de cómo múltiples veces los sistemas de autenticación niegan a un usuario legítimo como un usuario impostor. Esto también se conoce como tasa de no coincidencia falsa (FNMR), que se calcula mediante la fórmula que se indica a continuación

ERR (Equal Error Rate): este valor de parámetro muestra que el saldo de aceptaciones falsas está relacionado con el saldo de rechazos falsos. Cuanto menor sea el valor de la tasa de error igual, mayor será el rendimiento del sistema de autenticación biométrica. La tasa de error igual también se sugiere como tasa de cruce o tasa de error de cruce. El EER es calculado por de la siguiente manera.

Figura 14

Sensores biométricos a través de métricas

$$\text{FAR (\%)} = \frac{\text{Number of false accept}}{\text{number of imposters tested}} \times 100$$

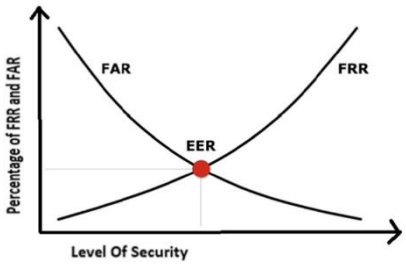
False Acceptance Rate (FAR)

$$\text{FRR (\%)} = \frac{\text{Number of rejections}}{\text{total number of users tested}} \times 100$$

False Rejection Rate (FRR)

$$\text{EER} = \text{FAR where FAR} = \text{FRR}$$

Equal Error Rate (EER)



FRR and FAR versus the level of security of a biometric authentication system plot

Nota. De "A review on performance, security and various biometric template protection schemes for biometric authentication systems". Por Sarkar & Singh, 2020.

En la tabla 14, mostramos un análisis de los diferentes tipos de sensores biométricos, clasificados por tipo y modo con una calificación de cada criterio de evaluación.

Tabla 14

Análisis de sensores biométricos fisiológicos y conductuales

Análisis de sensores biométricos fisiológicos y conductuales										
Tipo de Biometría	Modo biométrico	Sensor	Seguridad	Exactitud	Eficiencia	Usabilidad	Privacidad	Costo	FRR	FRVT
Fisiológica	Fingerprint	Camera	M	H	H	H	M	L	1%	
	Palmprint	Camera	M	H	M	M			3%	
	Hand geometry	Camera	M	M		M			<10%	
	Face	Camera	M	M	H	H	L	H	6%	87%
	Eye	Camera	H	H	M	M	L	H	<1%	
	Ear	Camera/Microphone	M	M		L			7%	
	ECG	Lead I type electrodes	H	H		M			5% - 18%	
Conductual	Tapping Behavior/keystroke	Touch screen	H	H	M	L		L	7% - 20%	
	Finger gesture	Touch screen	M	M	M	L			10%	
	Hand gesture	Accelerator, 3D camera	H	M		L			5% - 15%	
	Voice	Microphone	H	L		H		M	3%	
	Gait pattern	Wearable camera, accelerator	M	M		H			>6%	
	Daily routine activity	Wifi	M	M		L			>10%	

El FAR, FRR y ERR. Cuanto menor sea EER, mayor será la capacidad del método de autenticación biométrica para detectar a usuarios legítimos y prevenir intrusiones.

Tabla 15

Definición de criterios y niveles para las métricas

Criteria	Levels		
	High	**Medium**	**Low**
FAR, FRR, or EER	The experimental results of FAR, FRR or EER is less than 3%	The experimental results of FAR, FRR or EER is between 3% and 10%	The experimental results of FAR, FRR or EER is more than 10%
Efficiency	The time cost is less than 1 second. Or it is mentioned that the algorithm only costs a very little time, which implies that the method's computational cost is low, so that it is suitable to be implemented in a mobile device.	The time cost is between 1 and 3 seconds. Or the method needs a process of training and learning, but his method's computa- tional requirement is medium, thus may be possible but not very suitable to be implemented in a mobile device.	The time cost is more than 3 seconds. Or the method is usually implemented in a capable system, and needs a process of training and learning, which implies that the computational cost of this method is high, thus not suitable to be implemented in a mobile device.
Universality	Everyone has the underlying biometric fea- ture, which is not affected by disability, disease, and accident.	There is a small probability that the biometric feature might be affected by some accidents, e.g., the mute cannot use voiceprint authentication systems.	A large proportion of users do not have this feature.
Uniqueness	All human beings behave differently on the feature (i.e., the feature can uniquely represent every user's identity and be used in authentication).	The underlying feature is different in a large scale (e.g., the probability of two people having the same feature is less than 0.001%).	The feature is only different in a small scale (e.g., the probability of two people having the same feature is less than 0.1%).
Permanence	The biometric feature does not change in a user's whole lifetime.	The feature does not change distinctly in several years.	The feature may change significantly in a short period.
Acceptability	According to the result of searching in the Internet and our own experiences, the un- derlying biometric feature has been widely used in authentication in industry and busi- ness.	A biometric authentication has already been implemented, but it has not been widely used (i.e., the number of searching results is less than a million).	There are few examples of practical appli- cations.
Security	A security solution has been proposed with sound proof.	The biometric feature itself has a security characteristic that it is relatively difficult to attack. Or the proposal has briefly dis- cussed security issue.	There are few studies on the security issue. Or the biometric feature itself is not secure.
MSR	The percentage of MSR ≥ 90%	50% ≤ Thepercentageof MSR < 90%	Thepercentageof MSR < 50%

*Nota.*De "A Survey on Biometric Authentication: Towards Secure and Privacy-Preserving Identification". Por Zhang y Zheng, 2019.

Criteria	Total Scores		
	H	**M**	**L**
Accuracy	ts=9	6 ≤ ts ≤ 8	1 ≤ ts ≤ 5
Efficiency	ts=3	ts=2	ts=1
Usability	13 ≤ ts ≤ 15	8 ≤ ts ≤ 12	1 ≤ ts ≤ 7
Security	ts=3	ts=2	ts=1
Privacy	4 ≤ ts ≤ 6	2 ≤ ts ≤ 3	ts=1

Tabla 16

Resumen de los sistemas de autenticación biométrica existentes con características estáticas

References	Methods	Accuracy			Efficiency	Usability					Security	Privacy			
		FAR	FRR	EER		UV	UQ	PM	AC	EE		MSR	NI	RV	UL
[11]	Point distribution model	1	1	1	-	3	1	1	3	3	1	-	×	×	-
[12]	Surface Interpenetration Measure	3	2	2	2	3	1	1	3	2	3	-	-	-	-
[13]	Multiobjective evolution	1	1	1	-	3	1	1	3	3	1	-	-	-	-
[14]	iProov	2	2	2	3	3	1	1	3	3	3	-	-	-	C
[15]	Random projections	3	3	3	-	2	3	3	1	1	2	-	C	-	-
[17]	Visible sensing	3	3	3	-	2	3	3	1	1	2	-	-	-	-
[16]	-	3	3	3	-	2	3	3	1	1	2	-	-	-	-
[18]	Pupil dynamics	3	3	3	-	2	3	3	1	1	3	-	-	-	-
[19]	Biometric smart card	3	3	3	1	2	3	3	1	1	2	-	-	C	-
[20]	Eye movement tracking	2	2	2	-	2	3	3	1	1	2	-	-	-	-
[21]	The variation in pupil size	3	3	3	2	2	3	3	1	1	2	-	-	-	-
[34]	Delaunay quadrangle	-	-	-	-	2	3	3	3	3	2	-	-	-	-
[25]	Shift and rotation invariant feature extraction	3	3	3	3	2	3	3	3	3	-	-	-	-	-
[24]	-	3	3	3	3	2	3	3	3	3	-	-	-	-	-
[26]	Thermal images	3	3	3	-	2	3	3	3	1	3	-	-	-	-
[27]	Spectroscopic approach	-	-	-	-	2	3	3	3	1	3	-	-	-	-
[28]	Finger vein biometric	3	2	2	2	2	3	3	3	1	3	-	-	-	-
[29]	Finger odor	2	2	2	-	2	3	3	3	1	3	-	-	-	-
[30]	Hyperspectral imagery	2	2	2	-	2	3	3	3	1	3	-	-	-	-
[32]	Data hiding	3	3	3	-	2	3	3	3	3	1	-	×	C	×
[33]	Template synthesis	3	3	3	-	2	3	3	3	3	1	1	C	C	C
[35]	-	-	-	-	-	3	1	1	3	2	3	-	-	-	-
[36]	-	2	2	2	-	3	1	1	3	2	3	-	-	-	-
[37]	Fiducial point dependent method, Fiducial points independent method	3	3	3	-	3	1	1	3	2	3	-	-	-	-
[38]	HMM	3	1	1	-	3	3	2	3	3	3	-	-	-	-
[39]	HMM-GMM	2	2	2	-	3	3	2	3	3	1	-	-	-	-
[10]	-	3	1	1	-	3	3	2	3	3	3	-	-	-	-
[40]	PNN analytical method	3	3	3	-	2	1	1	1	1	2	-	-	-	-
[41]	-	2	2	2	-	2	1	1	1	1	2	-	-	-	-
[42]	Nearest neighbor, Neural network, Support vector machine, Random forest	2	2	2	-	2	1	1	1	1	2	-	-	-	-

C:The scheme in this article supports this criterion;
×:The scheme in this article does not support this criterion.

Nota. De "A Survey on Biometric Authentication: Towards Secure and Privacy-Preserving Identification". Por Zhang y Zheng, 2019.

Métrica: Para el desarrollo de la arquitectura biométrica y Cloud, se seleccionó como métrica principal la disponibilidad del servicio.

4.2.3 Análisis biométrico del tipo reconocimiento facial y de Iris según la FRVT e ICE de NIST.

Tabla 17

Face Recognition Vendor Test (FRVT)

FRVT en función de (arousal-valence) Electromyography (EMG) y Photoplethysmography (PPG)	
Emociones	**Precisión**
Angustia	92
Asco	87
Triste	84
Ansioso	90
Enojado	87
Impaciente	86
Preocupado	82
Aburrido	86
Asombrado	88
Convencido	85
Seguro	86
Grave	87
Entusiasmado	91
Contento	85
Complacido	88
Calma	93

Tabla 18

Análisis del impacto de la biometría fisiológica y conductual en función los papers revisados dentro del Q1-Q2 para nuestra investigación

Tipo de Biometría	Biometría	Sensor	Seguridad	Precisión	Eficiencia	Usabilidad	Privacidad	Costo	FRR
Fisiológica	Huella dactilar	cámara	M	H	H	H	M	L	1%
	Impresión de la palma	cámara	M	H	M	M			3%
	Geometría de la mano	Cámara	M	M		M			<10%
	Facial	Cámara	M	M	H	H	L	H	6%
	Iris	chamara	H	H	M	M	L	H	<1%
	Oído	cámara/Micrófono	M	M		L			7%
	ECG	Electrodos	H	H		M			5% - 18%
Conductual	Comportamiento de toque/pulsación de tecla	Pantalla táctil	H	H	M	L		L	7% - 20%
	Gesto con el dedo	Pantalla táctil	M	M	M	L			10%
	Gesto manual	Acelerador, cámara 3D	H	M		L			5% - 15%
	Voz	Micrófono	H	L		H		M	3%
	Patrón de caminata	Cámara portátil, acelerador.	M	M		H			>6%
	Actividad de rutina diaria	Wifi	M	M		L			>10%

Tabla 19

Métricas para la valorización de la precisión, eficiencia, usabilidad, seguridad, privacidad.

Validación	**Modelo**	**Precisión**			**Eficiencia**	**Usabilidad**					**Seguridad**	**Privacidad**			
Investigación	Mejora	FAR	FRR	EER	3	UV	UQ	PM	AC	EE	3	MSR	NI	RV	UL
		0	0.049%	0		3	3	3	2	3		2	1	1	1

El modelo aborda el análisis de los sensores biométricos fisiológicos o conductuales dando como mayor seguridad y precisión el reconocimiento de iris, está adaptada a la arquitectura Cloud con controles de la ISO 27001 para prevenir intrusiones.

4.2.4 Análisis de la de la Ley de Protección de datos Personales 29733 y el SGSI de la ISO 27001.

Tabla 20

Principios de la Ley de Protección de datos Personales 29733 y el SGSI de la ISO 27001

LPDP 29733				
PRINCIPIOS	**ISO 27001**			**DESCRIPCIÓN**
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	
Artículo 4. Principio de legalidad	X	X		Se prohíbe la recopilación de datos por medios Fraudulentos.
Artículo 5. Principio de consentimiento	X			Debe mediar el consentimiento del titular.
Artículo 6. Principio de finalidad	X	X		Deben ser recopilados para una finalidad determinada, explícita y lícita.
Artículo 7. Principio de proporcionalidad	X		X	Debe ser adecuado, relevante y no excesivo a la finalidad.
Artículo 8. Principio de calidad	X	X		Deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados; Deben conservarse de forma tal que se garantice su seguridad.

Artículo 9. Principio de seguridad	X	X	X	Deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad.
Artículo 10. Principio de disposición de recurso	X	X		Debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.
Artículo 11. Principio de nivel de protección adecuado	X	X	X	Debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar.
Artículo 12. Valor de los principios	X	X	X	Debe ajustarse a los principios rectores a que se refiere este título.
ARTÍCULOS	**ISO 27001**			**DESCRIPCIÓN**
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	
Artículo 3		X		Establece el principio de integridad, que requiere que los datos personales sean exactos, completos, actualizados y pertinentes en relación con la finalidad para la que fueron recopilados. Esto significa que los datos biométricos deben ser precisos y actualizados para garantizar su integridad.

Artículo 3	X			Establece el principio de confidencialidad, que requiere que los datos personales sean tratados con reserva y solo puedan ser revelados a terceros con el consentimiento del titular de los datos o en casos excepcionales previstos por la ley. En el caso de los datos biométricos, se deben adoptar medidas de seguridad adecuadas para garantizar su confidencialidad y prevenir su divulgación o acceso no autorizado.
Artículo 12			X	Dispone que se deben adoptar medidas de seguridad técnicas y organizativa adecuadas para garantizar la integridad de los datos personales y prevenir su alteración, pérdida, tratamiento o acceso no autorizado. Esto incluye medidas para garantizar la disponibilidad de los datos biométricos y prevenir su pérdida o destrucción.
Artículo 12	X			Dispone que se deben adoptar medidas de seguridad adecuadas para garantizar la confidencialidad de los datos personales y prevenir su divulgación o acceso no autorizado.
Artículo 12		X		Dispone que se deben adoptar medidas de seguridad técnicas y organizativas adecuadas para garantizar la integridad de los datos personales y prevenir su alteración, pérdida, tratamiento o acceso no autorizado.
Artículo 14			X	Dispone que el tratamiento de datos personales sensibles, como los datos biométricos, requiere el consentimiento expreso del titular de los datos, salvo en casos excepcionales previstos por la ley. Esto implica que se debe garantizar la confidencialidad de los datos biométricos y obtener el consentimiento expreso del titular para su tratamiento.

Artículo 18	X			Dispone que, en caso de una brecha de seguridad o violación de los datos personales, se debe notificar al titular de los datos afectado y adoptar medidas para preservar la confidencialidad de los datos.
Artículo 18			X	Dispone que, en caso de una brecha de seguridad o violación de los datos personales, se deben notificar al titular de los datos afectado y adoptar medidas para restaurar la disponibilidad de los datos.

4.2.5 Pilares del SGSI ISO 27001 para las arquitecturas Cloud

Tabla 21

Pilares del SGSI ISO 27001 para las arquitecturas Cloud

ISO 27001**- Biometría**					
ISO 27001	**RIESGOS**	**ISO /22301 SGCN**	**ISO / 27001**	**ISO / 27002**	**ISO/IEC 27032 ZERO TRUST**
CONFIDENCIALIDAD	La alteración o manipulación de los datos, la suplantación de identidad y el uso de datos biométricos falsos.	Cláusula 8.1.2: Análisis de riesgos, donde se deben identificar y evaluar los riesgos de seguridad, incluyendo la pérdida de confidencialidad de la información. Cláusula 8.2.1:	Cláusula A.7.1: Gestión de activos, donde se establecen los procedimientos para la identificación, clasificación y	Sección 10.1: Gestión de activos, donde se establecen los procedimientos para la identificación, clasificación y protección de los	Sección 6.3: Establecer controles de acceso y gestión de identidades y privilegios para asegurar que solamente las

		Establecimiento del sistema de gestión de la continuidad del negocio, que incluye la definición de políticas y procedimientos para garantizar la confidencialidad de la información.	protección de los activos relacionados con los datos biométricos. Cláusula A.18.1: Gestión de la seguridad de la información, que incluye la definición de políticas y procedimientos para garantizar la confidencialidad de la información.	activos relacionados con los datos biométricos. Sección 13.2: Seguridad de los equipos y dispositivos móviles, donde se establecen los procedimientos para garantizar la confidencialidad de los datos biométricos almacenados en dispositivos móviles.	personas autorizadas puedan acceder a los datos biométricos.

INTEGRIDAD	La pérdida de los datos, el fallo de los sistemas que los almacenan, la falta de redundancia y la falta de medidas de contingencia para garantizar la disponibilidad de los datos	Cláusula 6.1.2: Análisis de impacto en el negocio, donde se deben identificar los activos críticos y sus dependencias para garantizar su protección y continuidad. Cláusula 8.2.2: Planificación de la continuidad del negocio, que incluye la definición de objetivos y estrategias para mantener la integridad de los procesos y sistemas críticos	Cláusula A.12.1: Control de la documentación, que incluye la definición de los procedimientos y responsabilidades para garantizar la integridad de la documentación y registros relacionados con los datos biométricos. Cláusula A.12.6: Gestión de cambios, donde se establecen los procedimientos para gestionar los cambios en los procesos y sistemas que	Sección 12.1: Control de la documentación, donde se establecen los procedimientos para garantizar la integridad de la documentación y registros relacionados con los datos biométricos. Sección 12.5: Control de la información de la documentación, donde se establecen los procedimientos para garantizar la integridad de la información contenida en la documentación relacionada con los	Sección 6.1: Implementar medidas de seguridad y mejores prácticas para prevenir la alteración, destrucción o pérdida de datos críticos, incluyendo los datos biométricos.

			manejan datos biométricos.	datos biométricos.	
DISPONIBILIDAD	La interceptación de los datos durante la transmisión, la falta de controles de acceso adecuados y la fuga de datos a través de brechas de seguridad o incidentes de seguridad.	Cláusula 8.2.3: Implementación y operación del sistema de gestión de la continuidad del negocio, donde se deben definir los requisitos de disponibilidad y tiempos de recuperación de los sistemas y procesos críticos. Cláusula 8.3: Pruebas, revisión y mejora del sistema de gestión de la continuidad del negocio, que incluye la realización de pruebas de continuidad y la evaluación de los resultados para	Cláusula A.12.2: Control de los registros, que incluye la definición de los procedimientos para garantizar la disponibilidad de los registros y documentación relacionados con los datos biométricos. Cláusula A.16.1: Gestión de la continuidad del	Sección 12.2: Control de los registros, que incluye la definición de los procedimientos para garantizar la disponibilidad de los registros y documentación relacionados con los datos biométricos. Sección 14.1: Gestión de la disponibilidad, donde se establecen	Sección 6.4: Establecer planes de contingencia y de recuperación ante desastres para asegurar la disponibilidad continua de los sistemas y servicios que manejan datos biométricos

		mejorar la disponibilidad de los sistemas y procesos críticos.	negocio, donde se establecen los procedimientos para garantizar la disponibilidad de los procesos y sistemas que manejan datos biométricos.	los procedimientos para garantizar la disponibilidad de los procesos y sistemas que manejan datos biométricos.	

La investigación realizada proporciona una mayor seguridad en la autenticación y control de acceso para garantizar la integridad, confidencialidad y disponibilidad dentro de arquitecturas Cloud, reduciendo el riesgo de intrusiones y mejorando la protección de los datos sensibles en las organizaciones. Además, la arquitectura Cloud permite una mayor flexibilidad y escalabilidad en la gestión de los recursos informáticos de una organización.

4.3 Alcance de la solución

El alcance del uso del modelo de autenticación biométrica fisiológica o conductual para prevenir intrusiones usando Zero trust en arquitecturas Cloud se limita a casos de uso en plataformas Cloud, pero puede ser ampliado a más. Los usuarios han sido considerados como identidades, pero también las aplicaciones podrían ser consideradas; esto puede variar dependiendo de la organización y su estrategia de seguridad. Sin embargo, en general, se pueden utilizar en una amplia variedad de situaciones para mejorar la seguridad y la eficiencia de la gestión de identidad y acceso.

La autenticación multifactor existe, pero aún no es usado ampliamente. Después de la autenticación, ¿cuál es la garantía de que el usuario se abstendrá de realizar actividades maliciosas y riesgosas? Esto demuestra que las medidas de seguridad convencionales son estáticas y es necesario adoptar un enfoque que sea dinámico y adaptable al contexto.

Incorporamos el modelo Zero trust en Cloud que permita a las organizaciones proporcionar seguridad de acceso a sus recursos enfatizando "nunca confíes, siempre verifica". Está basado en tres principios: **verificar explícitamente** (autenticar y autorizar completamente cada solicitud antes de que se conceda el acceso), **acceso con privilegios mínimos** (autorizar a un usuario sólo con los derechos mínimos que requieren) y **asumir un incumplimiento** (las organizaciones pueden planificar capas adicionales de seguridad con esta mentalidad).

Como solución integral y confiable, la seguridad de identidad salvaguarda las identidades de una organización. Esto indica que, bajo ciertas circunstancias, cualquier identidad, ya sea un administrador de TI, un proveedor externo, un trabajador remoto, un dispositivo o una aplicación pueden convertirse en privilegiado, creando un vector de ataque para los activos más valiosos de una organización.

4.4 Diseño de la solución

Nivel de seguridad propuesto para la Autenticación Cloud (IAM)

Bader et al. (2021) alega que el uso de los procesos de autenticación y encriptación pueden asegurar la disponibilidad y la confidencialidad de la data.

Figura 15

Safety in Cloud Computing

Nota. Safety in Cloud Computing. De "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategieset". Por Bader et al., 2021. (https://ieeexplore.ieee.org/document/9404177)

Identity Access Management (IAM) opera los mecanismos del control de accesos y el sistema de gestión de identidad. IAM ofrece medidas de seguridad para mejorar la protección de los datos y la privacidad de los usuarios.

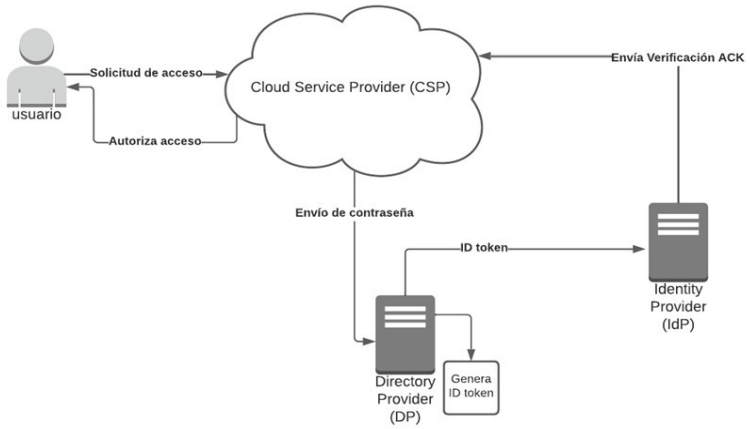
La capa o el nivel de seguridad empleado en nuestra propuesta Cloud está asociado a la seguridad de las aplicaciones, donde se quiere proteger las aplicaciones que se ejecutan en la nube para mitigar vulnerabilidades y ataques. Las medidas de seguridad que se usan para la propuesta son la autenticación multifactor (MFA) y el control de accesos basado en roles. El nivel de seguridad usado para los usuarios en Google Cloud IAM es la autenticación multifactor (MFA), que agrega una capa adicional de seguridad al proceso de inicio de sesión. Esto significa que, además de ingresar la contraseña, los usuarios deberán proporcionar un segundo factor de autenticación, como un código enviado a su teléfono móvil o, para nuestro caso dentro de las pruebas, su registro facial.

El otro nivel de seguridad importante revisado en la propuesta es el control de acceso basado en roles (RBAC), que permite a los usuarios definir roles y permisos para diferentes usuarios y grupos. Esto significa que los usuarios solo tendrán acceso a los recursos y datos que necesitan para realizar su trabajo, lo que reduce el riesgo de errores y vulnerabilidades.

4.4.1 Arquitectura Cloud.

Figura 16

Arquitectura Cloud - En función a la ISO 27001-2 para el control de riesgos criterios

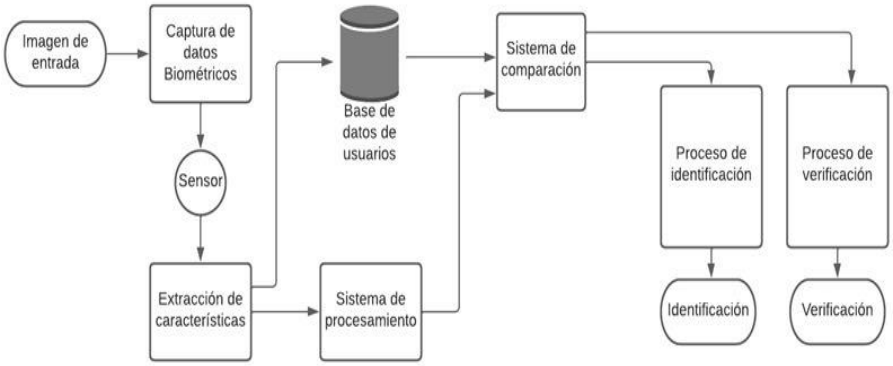


Nota. Adaptado "Biometrics for Internet-of-Things Security: A Review". Por Yang et al., 2021. (https://www.mdpi.com/1424-8220/21/18/6163)

4.4.2 Arquitectura biométrica

Figura 17

Arquitectura Biométrica - En función a las buenas prácticas de a ISO 24761



Nota. Adaptado "Biometrics for Internet-of-Things Security: A Review". Por Yang et al., 2021. (https://www.mdpi.com/1424-8220/21/18/6163)

4.4.3 Construcción de la solución.

Para un mayor entendimiento de la solución, definiremos los siguientes términos a emplear:

- Proveedor de Directorio (DP) es una empresa o entidad que ofrece servicios de directorio activo para la gestión y administración de usuarios y recursos en una red informática.
- Un proveedor de identidad (IDP) es un servicio que autentica y autoriza a los usuarios para acceder a aplicaciones y recursos en línea.
- SAML es un protocolo de intercambio de información de autenticación y autorización entre diferentes sistemas. Permite la autenticación única (SSO) y la federación de identidad.
- Los proveedores de servicios de nube (CSP) son compañias que establecen nubes públicas, gestionan nubes privadas u ofrecen recursos de cloud computing según se soliciten, la cual contiene la infraestructura como servicio (IaaS), la plataforma como servicio (PaaS) y el software como servicio (SaaS).
- Single Sign-On (SSO) es un método de autenticación que permite a los usuarios acceder a múltiples aplicaciones y servicios con una sola identificación y contraseña.

Proponemos tener procesos de autenticación y autorización añadiendo un servidor adicional, denominado Proveedor de Directorio (DP), para autenticar aún más el usuario mediante la verificación de sus datos biométricos.

Ambos IdP y DP deben autenticar al usuario para otorgar o negar el acceso a los recursos de la nube. Por un lado, el IdP utiliza el lenguaje de marcado de aserción de seguridad (SAML) 2.0 protocolo para autenticar al usuario por sus credenciales (nombre de usuario y contraseña).

En pocas palabras, cuando el CSP recibe una solicitud de acceso a un servicio/recurso determinado proporcionado por la nube, solicita al IdP que autentique a ese usuario. Tan pronto como el IdP reciba dicha solicitud del CSP, redirige al usuario para que ingrese sus credenciales a través de la página de inicio de sesión para probar su identidad. Si las credenciales correctas son recibidas por IdP, se verificará la identidad del usuario. Entonces el CSP solicita al DP que autentique aún más el usuario, pero esta vez se hace a través de un método biométrico, el proveedor del directorio redirige al usuario para una prueba de identidad ingresando sus datos biométricos. La decisión final de verificación se basa en los

resultados obtenidos en ambas fases. Es decir, el CSP verifica la identidad del usuario en función de los datos recibidos de las tres partes (IdP, DP y usuario) antes de otorgar al usuario el acceso a la nube solicitada servicio y/o recurso.

4.4.4 Enfoques de acceso.

Existen diferentes tipos de usuarios en la nube, cada uno con necesidades y objetivos específicos. Nuestro enfoque está en el acceso de usuarios finales con el uso de políticas de acceso condicional para limitar el acceso de los usuarios finales solo a ciertos recursos o en ciertas circunstancias.

A continuación, se describen algunos de los principales tipos de usuarios:

1. Propietario: este tipo de usuario tiene acceso completo a todos los recursos y servicios, incluyendo la posibilidad de crear y eliminar proyectos, así como de gestionar usuarios y permisos.
2. Administrador: este tipo de usuario tiene permisos para gestionar usuarios y recursos dentro de un proyecto específico, pero no puede crear o eliminar proyectos.
3. Desarrollador: este tipo de usuario tiene permisos para crear y gestionar recursos específicos dentro de un proyecto, como máquinas virtuales, bases de datos o servicios de almacenamiento.
4. Usuario final: este tipo de usuario tiene acceso limitado a los recursos y servicios, normalmente para utilizar aplicaciones o servicios específicos que han sido creados por otros usuarios.

4.4.5 Procesos de autenticación y autorización propuestos.

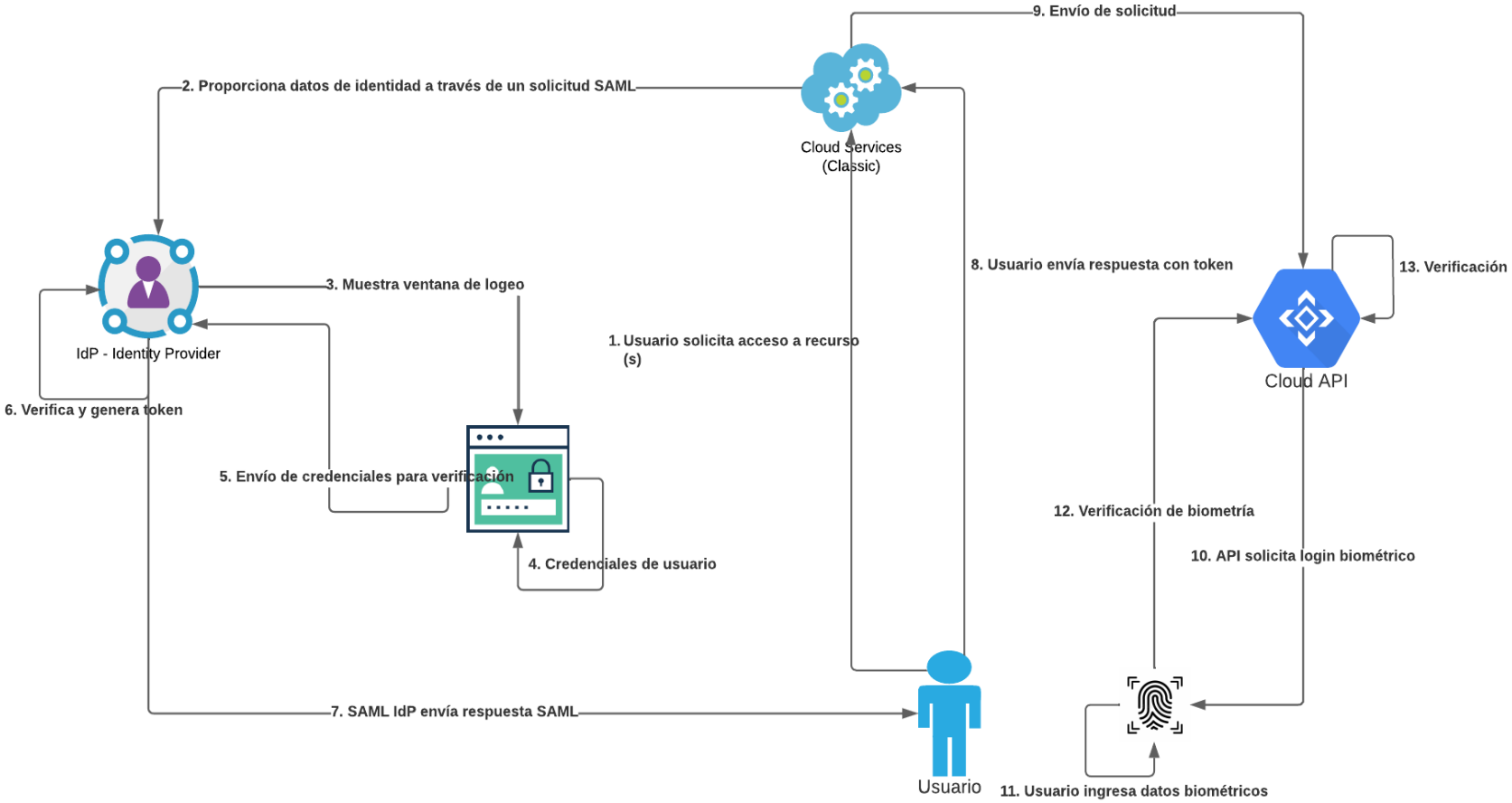
Proceso de autenticación

1. El proceso empieza cuando un usuario solicita acceso a un servicio/recurso proporcionado por el proveedor de servicios de una nube determinada (CSP), mediante el envío de una solicitud de acceso hacia él.
2. El CSP primero genera una solicitud SAML para el IdP para verificar la identidad del usuario.

3. El navegador ejecutado por el usuario es redirigido a un URL de inicio de sesión único (SSO) para recopilar las credenciales de usuario.
4. En este paso, el usuario ingresa sus credenciales, nombre de usuario y contraseña con el fin de obtener acceso al requerido servicio/recurso.
5. Las credenciales de usuario se envían al IdP para verificar los parámetros de identificación del usuario.
6. El IdP verifica las credenciales recibidas y genera un token de autenticación para el usuario en caso de que sean correctos. De lo contrario, se le negará el acceso al servicio/recurso requerido alojado por el CSP.
7. El Idp encripta el token para evitar cualquier exposición. La respuesta creada por SAML es enviada hacia el CSP y el token hacia el usuario.
8. La solicitud de autenticación es enviada por el usuario hacia el CSP usando el token.
9. Una vez el usuario pase la autenticación tradicional, una solicitud de acceso es enviada desde el CSP hacia el DP para realizar una segunda fase de autenticación. El CSP envía el token del usuario hacia el DP.
10. El DP solicita al usuario presentar su dato biométrico como un tercer factor de autenticación.
11. Los datos biométricos del usuario son almacenados.
12. Los datos biométricos del usuario son enviados hacia el DP como respuesta a la solicitud recibida.
13. El DP verifica los datos biométricos del usuario para confirmar su identidad.
14. Si los datos biométricos enviados por el usuario son verificados, una confirmación es enviada hacia el CSP, caso contrario se recibe un mensaje de negación.
15. El CSP realiza un proceso de validación de los 2 factores de autenticación recibidos tanto del Idp como del DP.
16. Si los 2 factores de autenticación son correctos el acceso al recurso/servicio es concedido, caso contrario es denegado.

Figura 18

Proceso de autenticación propuesto

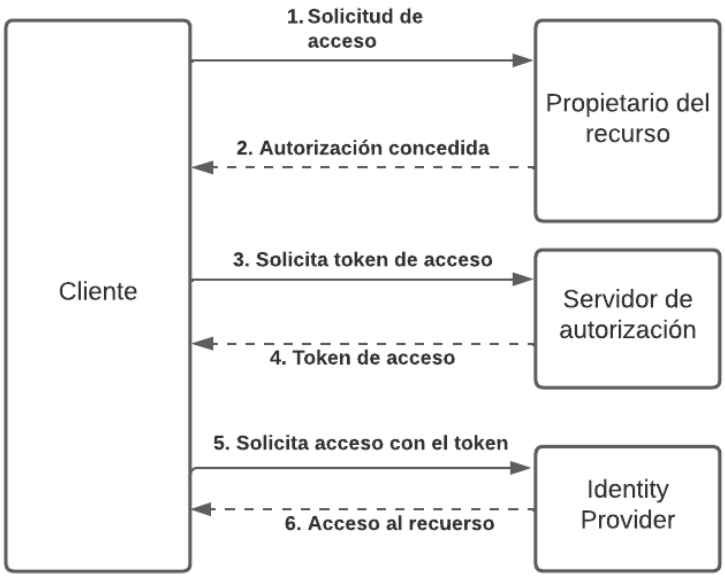


Proceso de autorización

1. El cliente solicita acceso a los datos que pertenecen al propietario del recurso.
2. El propietario del recurso responde enviando el permiso de autorización. La respuesta contiene, el tipo de autorización elegida, la autenticación preferible que se utilizará y cuál es el servidor que contiene los recursos.
3. El cliente reenvía la autorización al servidor de autenticación, solicitando el token de acceso.
4. El servidor de autenticación valida la concesión recibida y luego devuelve un token de acceso que representa al propietario del recurso y establece que se ha autorizado.
5. El cliente solicita permiso para acceder a los recursos protegidos desde el servidor que contiene los datos proporcionando el token de acceso.
6. El servidor de recursos recibe el token y lo valida, devolviendo los datos solicitados.

Figura 19

Proceso de autorización propuesto



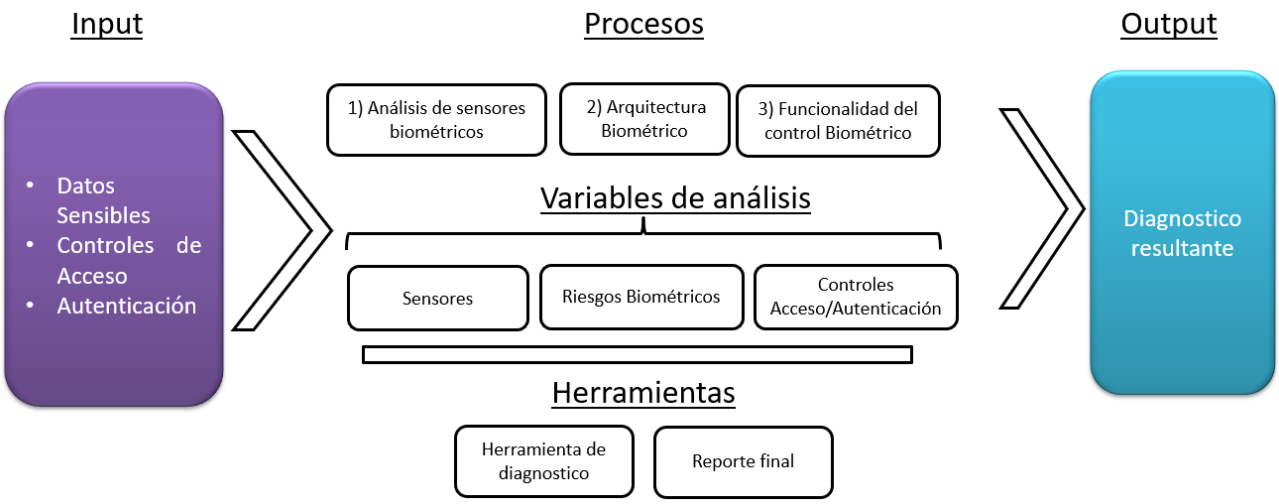
5. Desarrollo del artefacto

En este capítulo, desarrollamos un constructor que nos permitió elaborar un método para la creación de un modelo de autenticación biométrica fisiológica o conductual usando Zero Trust para prevenir intrusiones en arquitecturas Cloud.

En la siguiente figura, nos muestra los procesos que se realizó para la recolección de información.

Figura 20

Constructor



5.1.1 Diagnóstico resultante.

La investigación aborda la selección de sensores biométricos fisiológicos o conductuales con mayor valor en la seguridad y precisión (movimiento de labios e iris) para integrar a la arquitectura Cloud y Zero Trust, con la normalización de la ISO 27001 y la LPDP, que logre mitigar los riesgos de intrusiones en una arquitectura Cloud.

El diseño del modelo propuesto requiere verificación y análisis continuo de los servicios, aplicaciones y usuarios. Sólo después del proceso de verificación y sujeto a una disminución intervalo de tiempo se puede confiar a los elementos de la red para que accedan, utilicen e incluso modifiquen recursos dentro de los servicios Cloud.

Tabla 22

Componentes Zero trust para el modelo de autenticación propuesto.

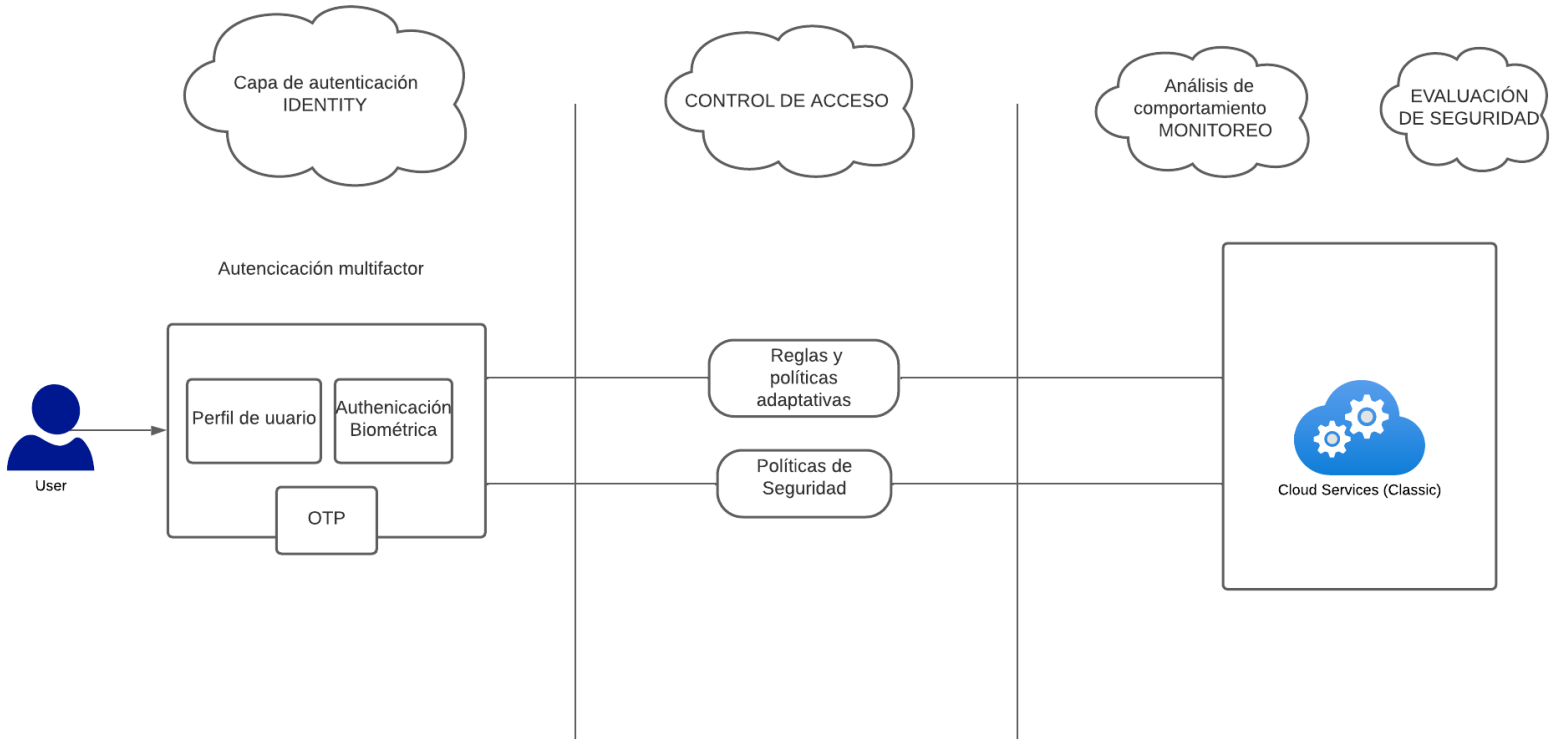
Componente	**Modelo Zero trust para Cloud**
Método de autenticación	Multifactor
Factores de autenticación	Fisiológicos, conductuales
Modelo de confianza	Zero Trust (nunca confiar, siempre verificar)
Política de seguridad	Políticas adaptativas
Gestión de seguridad	Visibilidad
Control de acceso	Control de acceso centralizado
Autenticación	Antes y durante

El modelo de autenticación Zero Trust hará uso de los sensores biométricos para lograr niveles elevados de autenticación. La arquitectura Zero Trust necesita un algoritmo que calcule la confianza. Este algoritmo decidirá si denegar o permitir cada solicitud individual de acceso y uso de los recursos Cloud. Un algoritmo de este tipo puede considerarse como una función con las entradas como atributos relevantes como el tipo de solicitud de acceso, el comportamiento previo de la entidad solicitante, historial de uso de recursos, historial previo de sanciones, políticas de IAM actuales, confianza del grupo al que pertenece la entidad.

Figura 21

Artefacto

Modelo de autenticación biométrica para prevenir intrusiones usando Zero trust para arquitecturas Cloud.



6. Protocolo de validación

6.1 Análisis de riesgos

En la integración de la autenticación biométrica, arquitectura Cloud, y Zero Trust se utilizan diversas métricas para evaluar la seguridad de los sistemas y redes, entre las que destaca la gestión de riesgos que mide y gestiona el riesgo en función de la actividad, la autenticación, los permisos y otros factores mencionados en el objetivo uno y dos. Se orquestan los controles de seguridad en tiempo real para mitigar los riesgos según la ISO 27001-2.

Tabla 23

Controles asociados a la ISO 27001-2

Controles asociados a la ISO 27001-2 para la validación de los riesgos de LPDP biométricos

Proceso(s): Autenticación Biométrica

Área: Control de Acceso a Plataforma Web

RIESGO Y ACTIVO			AMENAZA		Riesgo Inherente				TRATAMIENTO DEL RIESGO CON LA NORMA ISO 27001-2				Riesgo Residual			
Nº	Descripción del Riesgo (en función de la integridad, disponibilidad, confidencialidad)	Principales Activos afectados según la LPDP	Tipo	Descripción	Probabilidad	Impacto	Valor	Riesgo	Mecanismos de Protección Propuestos	Tipo de Control	Control Asociado	Tiempo Aprox.	Probabilidad	Impacto	Riesgo	Tolerancia
R1	Posible robo de identidad provoca daños de confidencialidad y privacidad por suplantación.	Afecta al derecho de privacidad y suplantación de identidad haciendo vulnerable	Amenazas Tecnológicas	Malware, Hacking o Cracking, Spoofing, pérdida de datos, fallas de hardware, fallas de red.	3	5	15	Critico	Definir una subred segura	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	C	2	1	2	Aceptado
			Amenazas en Instalaciones	Fuego o incendios, fallas mecánicas, fallas eléctricas, daño por fugas de agua.	1	5	5	Apreciable	Capacitaciones en protección ante riesgos físicos, desastres naturales	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	M	2	1	2	Aceptado
			Amenazas operacionales	Suplantación de identidad física, Sabotaje	3	5	15	Critico	Autenticación física supervisada, tráfico de red supervisado	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	C	2	1	2	Aceptado

RIESGO Y ACTIVO			AMENAZA		Riesgo Inherente				TRATAMIENTO DEL RIESGO CON LA NORMA ISO 27001-2				Riesgo Residual			
N°	Descripción del Riesgo (en función de la integridad, disponibilidad, confidencialidad)	Principales Activos afectados según la LPDP	Tipo	Descripción	Probabilidad	Impacto	Valor	Riesgo	Mecanismos de Protección Propuestos	Tipo de Control	Control Asociado	Tiempo Aprox.	Probabilidad	Impacto	Riesgo	Tolerancia
R2	Posible robo de datos biométricos provoca daños de integridad en el control de autenticación por obtención de datos.	Utilización de mecanismos de obtención de datos biométricos	Amenazas Tecnológicas	Malware, Hacking o Cracking, Spoofing, pérdida de datos, fallas de hardware, fallas de red.	3	5	15	Critico	Definir una subred segura	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	C	2	1	2	Aceptado
			Amenazas en Instalaciones	Fuego o incendios, fallas mecánicas, fallas eléctricas, daño por fugas de agua.	1	5	5	Apreciable	Capacitaciones en protección ante riesgos físicos, desastres naturales	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	M	2	1	2	Aceptado
			Amenazas operacionales	Suplantación de identidad física, Sabotaje	3	5	15	Critico	Autenticación física supervisada, tráfico de red supervisado	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	C	2	1	2	Aceptado

RIESGO Y ACTIVO			AMENAZA		Riesgo Inherente				TRATAMIENTO DEL RIESGO CON LA NORMA ISO 27001-2				Riesgo Residual			
N°	Descripción del Riesgo (en función de la integridad, disponibilidad, confidencialidad)	Principales Activos afectados según la LPDP	Tipo	Descripción	Probabilidad	Impacto	Valor	Riesgo	Mecanismos de Protección Propuestos	Tipo de Control	Control Asociado	Tiempo Aprox.	Probabilidad	Impacto	Riesgo	Tolerancia
R3	Posible pérdida de identidad provoca daños de confidencialidad, integridad y disponibilidad por la discapacidad o por la imposibilidad del uso biométrico	Afectación de la identidad por discapacidad o por imposibilidad	Amenazas Tecnológicas	Malware, Hacking o Cracking, Spoofing, pérdida de datos, fallas de hardware, fallas de red.	1	3	3	Apreciable	Definir una subred segura	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	C	2	1	2	Aceptado
			Amenazas Tecnológicas	Fuego o incendios, fallas mecánicas, fallas eléctricas, daño por fugas de agua.	3	5	15	Critico	Capacitaciones en protección ante riesgos fisicos, desastres naturales	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	C	2	1	2	Aceptado
			Amenazas operacionales	Suplantación de identidad fisica, Sabotaje	3	5	15	Critico	Autenticación fisica supervisada, tráfico de red supervisado	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	C	2	1	2	Aceptado

Tabla 24

Tratamiento del Riesgo con la Norma ISO 27001-2

TRATAMIENTO DEL RIESGO CON LA NORMA ISO 27001-2							
				Riesgo Residual			
Mecanismos de Protección Propuestos	Tipo de Control	Control Asociado	Tiempo Aprox.	Probabilidad	Impacto	Riesgo	Tolerancia
Definir una subred segura	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	C	2	1	2	Aceptado
Capacitaciones en protección ante riesgos fisicos, desastres naturales	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	M	2	1	2	Aceptado
Autenticación fisica supervisada, tráfico de red supervisado	Reducir	A.9.1.1,A.9.1.2,A.9.1.3,A.9.1.4,A.9.1.5,A.9.1.6, A.9.3.1,A.9.4.2,A.9.4.3,A.9.4.4,A.9.4.5,A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.2,A.12.4.3,A.12.4.4,A.17.1.1,A.17.1.2,A.17.1.3, A.15.2.1, A.14.2.2,A.14.2.3,A.14.2.4,A.14.2.5,A.14.2.6,A.14.2.7,A.14.2.8	C	2	1	2	Aceptado

		Probabilidad				
		1	2	3	4	5
Impacto	5					
	4					
	3					
	2					
	1		R1, R2, R3			

Critico	15 - 25
Importante	9-14
Apreciable	3- 8
Aceptado	1 - 2

6.2 Modelo de madurez

Se determinó el nivel de madurez a través de la evaluación de la seguridad, precisión del sensor y los controles de seguridad recomendados por la ISO 27001, ZTA y la LPDP a través del modelo de autenticación biométrica fisiológica o conductual para prevenir intrusiones en arquitecturas Cloud. El objetivo es avanzar de un nivel a otro, mejorando gradualmente la postura de seguridad y la capacidad de gestión de riesgos para la biometría fisiológica o conductual que se integre a la arquitectura Cloud y Zero Trust.

Tabla 25

Análisis del impacto de la biometría fisiológica o conductual en función a papers que se encuentran dentro del Q1-Q2 para nuestra investigación.

Análisis del impacto de la biometría fisiológica y conductual en función papers que se encuentran dentro del Q1-Q2 para nuestra investigación										
Biometric Type	Biometric	Sensor	Security	Accuracy	Efficiency	Usability	Privacy	Cost	FRR	FRVT
Physiological	Fingerprint	Camera	M	H	H	H	M	L	1%	
	Palmprint	Camera	M	H	M	M			3%	
	Hand geometry	Camera	M	M		M			<10%	
	Face	Camera	M	M	H	H	L	H	6%	87%
	Eye	Camera	H	H	M	M	L	H	<1%	
	Ear	Camera/Microphone	M	M		L			7%	
	ECG	Lead I type electrodes	H	H		M			5% - 18%	
Behaviorial	Tapping Behavior/keystroke	Touch screen	H	H	M	L		L	7% - 20%	
	Finger gesture	Touch screen	M	M	M	L			10%	
	Hand gesture	Accelerator, 3D camera	H	M		L			5% - 15%	
	Voice	Microphone	H	L		H		M	3%	
	Gait pattern	Wearable camera, accelerator	M	M		H			>6%	
	Daily routine activity	Wifi	M	M		L			>10%	

Tabla 26

Face Recognition Vendor Tes (FRVT)

FRVT en función de (arousal-valence) Electromyography (EMG) y Photoplethysmography (PPG)	
Emotions	Accuracy
Distress	92
Disgust	87
Sad	84
Anxious	90
Annoyed	87
Impatient	86
Worried	82
Bored	86
Astonished	88
Convinced	85
Confident	86
Serious	87
Excited	91
Delighted	85
Pleased	88
Calm	93

Integración en la Arquitectura biométrica, Cloud y Zero Trust de la propuesta de investigación.

Tabla 27

Seguridad en la integración de la arquitectura Biométrica, Cloud, Zero Trust para los tres pilares del SGCI: Integridad, Disponibilidad y Confidencialidad

Seguridad en la integración de la arquitectura Biométrica, Cloud, Zero Trust para los tres pilares del SGCI: Integridad, Disponibilidad y Confidencialidad									
Biometric Type	Biometric	Security							
		Biometric	IAM -GCP		ZTA				LPDP
		Security	RBAC	MFA	Propietario	Administrador	Desarrollador	Usuario final	
Physiological	Fingerprint	M	✓	✓	✓	✓	✓	✓	✓
	Palmprint	M	✓	✓	✓	✓	✓	✓	✓
	Hand geometry	M	✓	✓	✓	✓	✓	✓	✓
	Face	M	✓	✓	✓	✓	✓	✓	✓
	Eye	H	✓	✓	✓	✓	✓	✓	✓
	Ear	M	✓	✓	✓	✓	✓	✓	✓
	ECG	H	✓	✓	✓	✓	✓	✓	✓
Behaviorial	Tapping Behavior/keystroke	H	✓	✓	✓	✓	✓	✓	✓
	Finger gesture	M	✓	✓	✓	✓	✓	✓	✓
	Hand gesture	H	✓	✓	✓	✓	✓	✓	✓
	Voice	H	✓	✓	✓	✓	✓	✓	✓
	Gait pattern	M	✓	✓	✓	✓	✓	✓	✓
	Daily routine activity	M	✓	✓	✓	✓	✓	✓	✓

Tabla 28

Matriz de correspondencia entre los niveles de madurez de los tres marcos de referencia (NIST, ZTA e ISO 27001) para el método de autenticación biométrica fisiológica o conductual para prevenir intrusiones en una arquitectura Cloud.

Matriz de correspondencia entre los niveles de madurez de los tres marcos de referencia (NIST, ZTA e ISO 27001) para el método de autenticación biométrica fisiológica o conductual para mitigar intrusiones en una infraestructura Cloud.

Nivel	Nivel de madurez según NIST en biometriá conductual y fisiologica
1	**Sistema de autenticación biométrica básico:** El sistema solo recopila y utiliza una única modalidad biométrica para la autenticación, como el reconocimiento de la huella dactilar o la identificación de la voz. El sistema no está diseñado para resistir ataques o fraudes de alta complejidad.
2	**Sistema de autenticación biométrica básico con capacidad de detección de presentación falsa:** Además de la autenticación biométrica, el sistema puede detectar si la muestra biométrica presentada es genuina o se trata de una réplica, copia o imagen en 2D/3D de la misma. El sistema es más resistente a ataques y fraudes, pero sigue siendo vulnerable a ciertos tipos de ataques.
3	**Sistema de autenticación biométrica moderadamente avanzado:** El sistema es capaz de utilizar múltiples modalidades biométricas y puede detectar presentaciones falsas avanzadas, como máscaras o modelos en 3D. El sistema es más resistente a ataques y fraudes que los sistemas de nivel inferior.
4	**Sistema de autenticación biométrica avanzado:** El sistema puede utilizar múltiples modalidades biométricas, detectar presentaciones falsas avanzadas y tiene mecanismos de protección contra ataques sofisticados, como la suplantación de identidad mediante la combinación de varias modalidades biométricas. Además, el sistema es capaz de adaptarse a las características biométricas cambiantes de los usuarios, como el envejecimiento o el uso de accesorios (gafas, sombrero, etc.). El sistema es altamente resistente a ataques y fraudes y es adecuado para aplicaciones críticas de seguridad.
5	**Sistema de autenticación biométrica adaptativo:** El sistema es capaz de ajustar automáticamente sus parámetros de autenticación en función de la situación y del perfil de usuario, como la probabilidad de que el usuario presente características biométricas cambiantes o la criticidad de la transacción. Además, el sistema puede realizar una evaluación continua del riesgo de autenticación, actualizando la probabilidad de que el usuario sea quien dice ser en función de la información contextual, ambiental o de comportamiento. El sistema es altamente resistente a ataques y fraudes y es adecuado para aplicaciones críticas de seguridad en entornos cambiantes y dinámicos.

Nivel	Nivel de madurez según ZTA (Zero Trust Architecture)
1	En este nivel, la organización no cuenta con un sistema de autenticación biométrica fisiológica o conductual implementado. La autenticación se realiza a través de contraseñas o algún otro método de autenticación básico.
2	En este nivel, la organización ha implementado un sistema de autenticación biométrica fisiológica o conductual de baja calidad. Además, se han implementado algunos controles de seguridad basados en Zero Trust, como la autenticación multifactor y la segmentación de red.
3	En este nivel, la organización ha implementado un sistema de autenticación biométrica de alta calidad. Además, se han implementado controles de seguridad adicionales, como la verificación continua de usuarios y dispositivos biométricos y la detección de amenazas en tiempo real.
4	En este nivel, la organización ha implementado un sistema de autenticación biométrica resistente a la suplantación con detección de presentación. Además, se han implementado controles de seguridad avanzados, como la orquestación de políticas de seguridad en tiempo real y la automatización de la respuesta a incidentes.
5	En este nivel, la organización ha alcanzado un alto nivel de madurez en la integración de la autenticación biométrica fisiológica o conductual en la arquitectura de Zero Trust en la nube. Además, ha implementado controles de seguridad avanzados, como la orquestación de políticas de seguridad en tiempo real y la automatización de la respuesta a incidentes. La organización cuenta con un equipo dedicado a la ciberseguridad y realiza evaluaciones regulares de la efectividad de los controles de seguridad implementados.

Nivel	Nivel de Madurez según la ISO 27001
1	Cumplimiento de la legislación obligatoria.
2	Evaluación del proceso de Gestión de Seguridad.
3	Analizar el riesgo y la gestión de su resolución.
4	Adquisición de productos para integrarlos en los Sistemas de Gestión.
5	Integración de los componentes certificados en sistemas compuestos y su certificación.

Tabla 29

Nivel de madurez para el método de autenticación biométrica fisiológica o conductual para prevenir intrusiones en una arquitectura Cloud

Nivel de madurez para el método de autenticación biométrica fisiológica o conductual que mitiga intrusiones en una infraestructura Cloud	
Biometría Fisiológica	
Huella dactilar	4
Palma de la mano	3
Geometría de la mano	2
Rostro	4
Iris	3
Oreja	2
Electrocardiograma	4
Biometría Conductual	**Nivel**
Comportamiento de pulsaciones / Tecleo	3
Gesto de dedos	4
Gesto de manos	3
Voz	4
Patrones de movimiento	2
Actividad rutinaria diaria	2

Figura 22

Nivel de madurez de la biometría fisiológica

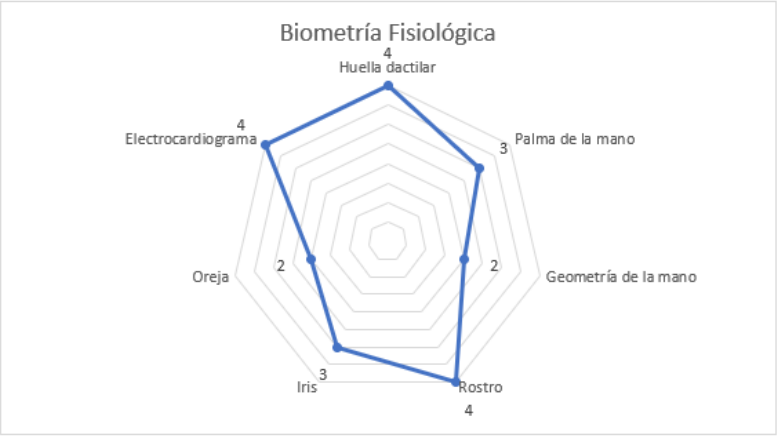


Figura 23

Nivel de madurez de la biometría conductual

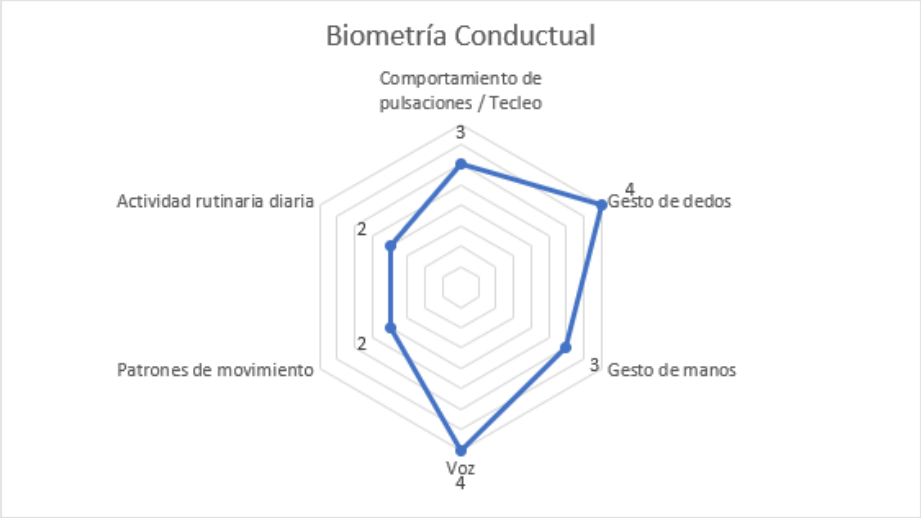


Tabla 30

Visibilidad en la norma ISO 22301 para la integración de la continuidad del negocio en la planificación estratégica y operativa de la organización: User Authentication on Mobile Device

Visibilidad en la norma ISO 22301 para la integración de la continuidad del negocio en la planificación estratégica y operativa de la organización						
User Authentication on Mobile Device						
Knowledge		Physiological biometics	Behavioral biometrics	Two/Multi factor		
Text based Secret	Graphical Secret	Fingerprint	Tapping behavior	Traditional Two/Multiple Factors	Ownership based Two Factors	Advanced Two/Multiple Factors
PIN	Recall based graphical password (e.g. Lock pattern, free form gesture)	Palmprint	Finger gesture	Combine different biometic factors based on sensor fusion	Knowledge + Owership	Integrating Knowledge factors with biometric factors and ownership factors
Password	Recognition based graphical password (e.g. graph, pixels)	Hand geometry	Hand gesture	Combine knowledge and biometrics	Biometrics + Ownership	
		Face	Voice			
		Eye	Gait			
		Ear	Daily routine activity			
		ECG, EEG				

Tabla 31

Visibilidad en la norma ISO 22301 para la integración de la continuidad del negocio en la planificación estratégica y operativa de la organización: Authentication Techniques

Visibilidad en la norma ISO 22301 para la integración de la continuidad del negocio en la planificación estratégica y operativa de la organización						
Authentication Techniques						
Shared Secrets	One Time Pasword	Token		Intrinsic Authentication	Behavioral	Next Generation
Static Password	Time based	**Software**	**Hardware**	Human Properties	Localization Metadata	FIDO
	Challenge Response Based	SSL/Certificate Exchange	Connected Tokens	Silicon Properties		CryptoPhoto
	Out of band Tranmission	Key Exchange	- Smart Cards			Blockchain
	Lockstep based	Third party	- USB Keys			
			- Key fob			
			Connectless Tokens			
			Disconnected Tokens			

6.3 Plan de implementación

Para la validación de la arquitectura se consideró los siguientes criterios.

Tabla 32

Plan de implementación

Diagrama de Gantt																	
Problemática	**Actividades**	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8	Semana 9	Semana 10	Semana 11	Semana 12	Semana 13	Semana 14	Semana 15	Semana 16
Identificar el problema y motivación/ Mostrar la Importancia del estudio	Antecedentes y la identificación del problema																
	Lectura de Papers en base y selección en Q1																
	Matriz de conocimiento para generar aporte dentro de nuestra investigación																
	Desarrollo de los objetivos para abordar la problemática																
Objetivos específicos	**Actividades**																
Analizar sensores biométrico fisiológico o conductual que permita prevenir intrusiones; basado en la Ley de Protección de Datos Personales (LPDP) y las normas de la Organización Internacional de	Analizar la Ley de protección de datos personales en función a la privacidad, disponibilidad de la información vs la Norma ISO para la integración de la Biometría.																
	Analizar los tipos de sensores biométricos fisiológicos o conductuales, para el tratamiento y el desarrollo de la propuesta en función a criterios.																
	Analizar la disponibilidad de equipos biométricos fisiológicos o conductuales en Perú																

Normalización (ISO).																	
	Diseñar una arquitectura Cloud Services Provider																
Diseñar un modelo de autenticación biométrica integrada a la arquitectura Cloud bajo el enfoque de Zero Trust para prevenir intrusiones de suplantación de identidades.	Diseñar una arquitectura biométrica con la ISO 24761																
	Evaluar la arquitectura de Zero Trust para la integración al desarrollo																
	Integrar las arquitecturas para apalancar la seguridad y esta de una segregación de autenticación en el escalamiento de prioridades del negocio																
	Proponer el método de autenticación para el control de accesos no autorizados.																
Evaluar el modelo de autenticación biométrica para prevenir intrusiones en arquitecturas Cloud basado en buenas prácticas de ciberseguridad. (NIST, ZTA e ISO 27001)	Validar el artefacto																
	Identificar los riesgos, amenazas posibles, mitigar los riesgos inherentes a residuales bajo controles de seguridad de la ISO																
	Evaluar la métrica en del desarrollo en la arquitectura por medio de preguntas para validar lo propuesto																
	Simulación en un war room de ciberseguridad la propuesta																
	Propuesta de continuidad de negocio y mejora de la investigación.																

6.4 Trabajos futuros

- Mejora de la precisión y la eficacia: Aunque los métodos de autenticación biométrica han mejorado significativamente en los últimos años, todavía hay margen de mejora en términos de precisión y eficacia. Los investigadores pueden trabajar en mejorar la capacidad de los sistemas biométricos para reconocer patrones fisiológicos o conductuales únicos de los usuarios y reducir los errores de autenticación. Mayor seguridad y protección de datos: A medida que los sistemas biométricos se vuelven más comunes, también aumenta el riesgo de ataques cibernéticos y la vulnerabilidad de los datos biométricos. Los investigadores pueden trabajar en desarrollar técnicas más avanzadas de encriptación y protección de datos para garantizar la seguridad de los datos biométricos.
- Integración con otras tecnologías de seguridad: Los sistemas de autenticación biométrica pueden ser más eficaces si se integran con otras tecnologías de seguridad, como la autenticación multifactorial, la detección de intrusiones y la criptografía. Los investigadores pueden trabajar en desarrollar formas de integrar estos diferentes métodos de seguridad para proporcionar una mayor protección contra las intrusiones.
- Mejora de la usabilidad y la experiencia del usuario: Aunque los sistemas biométricos pueden proporcionar un alto nivel de seguridad, también pueden ser incómodos o confusos para los usuarios. Los investigadores pueden trabajar en desarrollar sistemas más fáciles de usar y más intuitivos que mejoren la experiencia del usuario.
- Investigación sobre nuevas tecnologías biométricas: A medida que avanza la tecnología, es probable que surjan nuevas formas de autenticación biométrica. Los investigadores pueden trabajar en la exploración de nuevas tecnologías, como la autenticación basada en el ADN o la autenticación basada en la voz, para ver si son viables como método de autenticación biométrica.
- Integración con tecnologías de inteligencia artificial (IA): La integración de la biometría con la IA podría mejorar la precisión y eficacia de los sistemas de autenticación biométrica. Los investigadores pueden trabajar en desarrollar modelos

de IA que sean capaces de detectar patrones biométricos y reducir los errores de autenticación.

Conclusiones

- El modelo de autenticación propuesto ofrece pasos prácticos para su implementación en arquitecturas Cloud. Esta investigación se centra en implementar el modelo Zero trust junto con la autenticación multifactor. Con los pasos descritos para su implementación, las organizaciones podrían reducir la superficie de ataque y mejorar significativamente su postura de seguridad Cloud.
- El modelo de autenticación biométrica fisiológica o conductual para prevenir intrusiones usando Zero trust en arquitecturas Cloud propuesto representa un aporte significativo para prevenir intrusiones en escenarios de suplantación de identidad, mediante un análisis de diversos métodos biométricos normalizados por la ISO 27001 y la Ley de protección de datos personales (LDPD).
- Esta investigación propone un modelo de autenticación que protege las identidades contra las amenazas cibernéticas considerando la identidad como un perímetro de seguridad. Se analizaron sensores biométricos fisiológicos y conductuales para prevenir intrusiones, siguiendo los principios establecidos por la ley de protección de datos personales (LDPD) y las normas de la organización internacional de normalización (ISO).
- Esta investigación permitió desarrollar un modelo basado en diagramas y diseños claros ayudando a comprender la escalabilidad del modelo propuesto con el objetivo de prevenir intrusiones en escenarios de suplantación de identidad para arquitecturas Cloud.
- Es necesario tomar medidas adicionales al implementar el modelo Zero Trust para una red, por ejemplo, controles de seguridad (segmentación de red), agrupación de usuarios y nodos basados en políticas de acceso, así como detección y respuesta de endpoints (EDR). La implementación de modelo Zero Trust se ha convertido es una necesidad crítica para las organizaciones debido al aumento del trabajo remoto y la dependencia del uso de servicios Cloud y los dispositivos IoT.

- Se evaluó el modelo de autenticación biométrica propuesta para prevenir intrusiones en arquitecturas Cloud basado en buenas prácticas de ciberseguridad. (NIST, ZTA e ISO 27001). Los resultados de los protocolos de validación, sección 6, brindan una mejor visibilidad, respaldando de manera sólida la viabilidad y efectividad del modelo de autenticación biométrica basado en características fisiológicas. Esta medida de seguridad adicional establece un enfoque de Zero Trust en el acceso a los recursos Cloud.

Recomendaciones

- Se recomienda segmentar y segregar las funciones de control de acceso y autenticación en el desarrollo de las arquitecturas Cloud con el fin de obtener una visibilidad holística.
- Antes de implementar la autenticación biométrica, arquitectura Cloud y Zero Trust, es importante realizar una evaluación de riesgos para identificar las posibles amenazas y riesgos asociados a los recursos que se desean proteger. Esto permitirá a la organización establecer los controles adecuados para mitigar los riesgos identificados.
- Es crucial seleccionar la tecnología adecuada para implementar una autenticación biométrica, arquitectura Cloud y Zero Trust. La tecnología seleccionada debe ser escalable, flexible y fácilmente integrable con otras tecnologías.
- Es necesario proporcionar capacitación a los usuarios sobre el uso de la autenticación biométrica y el acceso Zero Trust. Los usuarios deben estar informados sobre las políticas y prácticas de seguridad, así como los requisitos de autenticación necesarios para acceder a los recursos. Además, es importante integrar la autenticación biométrica con las políticas de seguridad existentes dentro de la organización para asegurar el cumplimiento de los requerimientos de seguridad en todo momento.
- Es importante tener en cuenta que la implementación de un sistema de autenticación biométrica también presenta desafíos. Por ejemplo, se deben tomar medidas para proteger los datos biométricos de los usuarios y evitar posibles vulnerabilidades.
- Se debe considerar la posibilidad de que algunos usuarios no puedan utilizar este sistema debido a limitaciones físicas o tecnológicas.
- Según la investigación realizada, se sugiere que la integración de la autenticación biométrica, arquitectura Cloud y Zero Trust se realice utilizando técnicas de autenticación como la FIDO, CryptoPhoto y Blockchain. Esto tiene

como objetivo garantizar la continuidad del negocio y facilitar futuras investigaciones.

Glosario

- LPDP – Es la Ley Orgánica de Protección de Datos Personales, cuya función es la protección de cada dato e información de cada ciudadano en contra de los abusos, el mal uso, los descuidos en los tratamientos a dichos datos realizados por terceros.
- ISO: Organización Internacional de Normalización. Es una organización independiente que desarrolla estándares internacionales para diversas industrias y áreas, incluyendo calidad, medio ambiente y seguridad de la información.
- NIST: Instituto Nacional de Estándares y Tecnología. Es una agencia gubernamental de los Estados Unidos que desarrolla y promueve estándares y guías para la ciencia, la tecnología y la seguridad cibernética.
- SGSI: Estas siglas hacen referencia al Sistema de Gestión de Seguridad de la Información. Este es un conjunto de cada política, proceso, procedimiento y control de seguridad que permite la protección de las informaciones de las organizaciones.
- PDCA: Planificar, Hacer, Verificar, Actuar. Es un ciclo de mejora continua utilizado en la gestión de la calidad y otros campos para mejorar los procesos y resultados.
- PICOC: Planificación, Identificación, Contención, Ofensiva, Cierre. Es un marco de respuesta a incidentes utilizado en la seguridad cibernética para abordar los incidentes de manera estructurada y efectiva.
- IAM: Gestión de Acceso e Identidad. Se refiere a la administración de identidades de usuarios y permisos de acceso para sistemas y aplicaciones.
- FAR: Tasa de Falsas Aceptaciones. Es la probabilidad de que un sistema de reconocimiento de biometría acepte una identificación falsa.
- FRR: Tasa de Falsos Rechazos. Es la probabilidad de que un sistema de reconocimiento de biometría rechace una identificación válida.
- EER: Tasa de Error de Igualación. Es la tasa en la que un sistema de reconocimiento de biometría acepta una identificación válida y rechaza una identificación falsa.

- API: Interfaz de Programación de Aplicaciones. Hace referencia al conjunto de cada protocolo y herramienta que contribuyen para que los desarrolladores creen aplicaciones que estarán comunicadas con otro sistema o servicio.
- OAuth: Protocolo de autorización abierto. Permite que una aplicación acceda a información protegida en nombre de un usuario sin que el usuario tenga que compartir sus credenciales de acceso directamente.
- ESET: Una empresa de seguridad informática que desarrolla software antivirus y soluciones de seguridad para dispositivos y redes.
- IBM: International Business Machines. Es una empresa de tecnología de la información y servicios de consultoría que ofrece soluciones de hardware, software y servicios en la nube.
- BEC: Compromiso de correo electrónico empresarial. Es un tipo de ataque de phishing en el que un atacante busca obtener acceso no autorizado a los sistemas empresariales y los datos confidenciales mediante el engaño de los usuarios.
- MFA: Autenticación multifactor. Se refiere al uso de múltiples factores de autenticación, como una contraseña y un código de verificación enviado por mensaje de texto, para mejorar la seguridad de la autenticación.
- CRM: Gestión de Relaciones con los Clientes. Se refiere a la administración de las interacciones con los clientes y la gestión de las relaciones con ellos para mejorar la satisfacción y la retención de los clientes.
- IaaS: Infraestructura como Servicio. Es un modelo de entrega en la nube en el que un proveedor de servicios de nube proporciona infraestructura informática, como servidores y almacenamiento, a través de Internet.
- PaaS: Plataforma como Servicio. Es un modelo de entrega en la nube en el que un proveedor de servicios de nube proporciona una plataforma de desarrollo y ejecución de aplicaciones, que incluye herramientas y servicios para crear, probar y desplegar aplicaciones.
- SaaS: Software como Servicio. Es un modelo de entrega en la nube en el que un proveedor de servicios de nube proporciona acceso a un software a través de

Internet, en lugar de que el usuario tenga que descargar e instalar el software en su computadora.

- TI: Tecnología de la Información. Se refiere al uso de tecnología para almacenar, procesar y transmitir información.
- NCCoE: Centro Nacional de Excelencia en Ciberseguridad de Estados Unidos. Es una iniciativa del gobierno de Estados Unidos que desarrolla soluciones de ciberseguridad y promueve las mejores prácticas en seguridad cibernética.
- ZTA: Acceso de Confianza Cero. Es un modelo de seguridad cibernética en el que se requiere una autenticación rigurosa y una verificación continua de la identidad y los dispositivos para acceder a los recursos.
- PDCA: Planificar, Hacer, Verificar, Actuar. Es un ciclo de mejora continua utilizado en la gestión de la calidad y otros campos para mejorar los procesos y resultados.
- DPI: Inspección Profunda de Paquetes. Es una técnica utilizada en redes de computadoras para analizar el contenido de los paquetes de datos que se envían y reciben.
- SGCN: Sistema de Gestión de la Continuidad del Negocio. Este, a través de la norma ISO 22301, contribuye a que cada empresa controle permanentemente cada riesgo que se ocasione en su negocio y tener conocimiento de la capacidad para prevenir un accidente o riesgo imprevisto con el que puede ser solucionado.
- IDS: Sistema de Detección de Intrusos. Es un sistema de seguridad cibernética que monitorea y analiza el tráfico de red para identificar posibles intrusiones o actividades maliciosas.
- IPS: Sistema de Prevención de Intrusos. Es un sistema de seguridad cibernética que, además de detectar posibles intrusiones, también tiene la capacidad de bloquear o impedir el acceso no autorizado.
- OTP: Contraseña de un solo uso. Es una contraseña que solo se puede utilizar una vez y que se genera automáticamente para cada inicio de sesión. Esto proporciona una capa adicional de seguridad, ya que incluso si un atacante obtiene la contraseña, no podrán utilizarla nuevamente.

- BaaS: Backend como Servicio. Es un modelo de entrega en la nube en el que un proveedor de servicios de nube proporciona la infraestructura y la plataforma para el backend de una aplicación, incluyendo almacenamiento de datos, autenticación de usuario y lógica de negocio.
- OWL: Lenguaje de Ontologías Web. Es un lenguaje de programación utilizado para describir las ontologías, que son una forma de representar el conocimiento y las relaciones entre conceptos.
- IoT: Internet de las cosas. Hace referencia a la conexión de cada dispositivo y objeto cotidiano a Internet, ello permitirá que se recopilen e intercambien datos con el fin de la mejora de la eficiencia y la automatización en cada campo, como un hogar inteligente, las industrias y la salud.
- CIS: Centro de Información de Seguridad. Es una organización sin fines de lucro que tiene como objetivo proporcionar recursos y herramientas para mejorar la seguridad cibernética en el sector público y privado.
- PCI: Industria de tarjetas de pago. Es un conjunto de normas de seguridad para la protección de los datos de las tarjetas de pago, establecidas por los principales proveedores de tarjetas de crédito y débito.
- DSS: Estándar de seguridad de datos para la industria de tarjetas de pago. Es un conjunto de requisitos para la protección de los datos de las tarjetas de pago que deben cumplir todas las empresas que procesan, transmiten o almacenan datos de tarjetas de pago.
- COBIT: Objetivos de control de la información y la tecnología relacionada. Es un marco de trabajo de gobierno y gestión de TI utilizado para garantizar la seguridad, la eficiencia y la efectividad de los sistemas de información y tecnología.
- DP: Protección de datos. Es un conjunto de medidas para garantizar la privacidad y seguridad de los datos personales, incluyendo su recolección, almacenamiento, procesamiento y transmisión.
- IdP: Proveedor de identidad. Es un sistema que permite a los usuarios autenticarse y autorizar el acceso a diferentes aplicaciones y servicios en línea utilizando un solo conjunto de credenciales.

- SAML: Lenguaje de marcado de atributos de seguridad. Es un estándar de seguridad para la autenticación y autorización de usuarios en aplicaciones y servicios en línea, que permite la transferencia segura de información de identidad y atributos entre el proveedor de identidad y el proveedor de servicios.
- CSP: Proveedor de servicios en la nube. Es una empresa que proporciona servicios de nube, como almacenamiento, procesamiento y análisis de datos, a través de Internet.
- URL: Localizador uniforme de recursos. Es una cadena de caracteres utilizada para identificar de manera única una ubicación en la web, como una página web o un archivo.
- SSO: Inicio de sesión único. Es una solución que permite a los usuarios iniciar sesión una sola vez y acceder a múltiples aplicaciones y servicios sin tener que volver a autenticarse.
- Mission Success Rate (MSR): Es la tasa de éxito de una misión o proyecto, que se mide en términos de cumplimiento de objetivos y requisitos.
- Non-invertibility (NI): Es una propiedad de los sistemas criptográficos que asegura que no es posible recuperar la clave original a partir de un mensaje cifrado sin conocer la clave de cifrado.
- Revocability (RV): Es la capacidad de revocar un permiso o acceso otorgado previamente. En seguridad de la información, se refiere a la capacidad de revocar un certificado o credencial en caso de que se haya comprometido o haya sido utilizado de manera indebida.
- Unlinkability (UL): Es la capacidad de separar y ocultar la relación entre dos conjuntos de datos o entidades, lo que dificulta la identificación y seguimiento de los usuarios o información.
- Universality (UV): Es la capacidad de un sistema biométrico para reconocer a cualquier persona en la población a la que está destinado, independientemente de su edad, género, raza, etc.

- Uniqueness (UQ): Es la capacidad de un sistema biométrico para distinguir de manera única a un individuo de todos los demás en la población a la que está destinado.
- Permanence (PM): Es la capacidad de un sistema biométrico para mantener su precisión y fiabilidad a lo largo del tiempo, a pesar de los cambios naturales en los rasgos biométricos del individuo.
- Acceptability (AC): Es la disposición de los usuarios a utilizar un sistema biométrico, lo que está influenciado por factores como la comodidad, la facilidad de uso, la privacidad y la confianza en la tecnología.
- Extra Equipment (EE): Es el equipo adicional necesario para realizar una tarea o función específica. En seguridad biométrica, se refiere a los dispositivos o instrumentos necesarios para adquirir y procesar los datos biométricos de un individuo.
- Ransomware: Es un tipo de software malicioso diseñado para bloquear el acceso a un sistema o a los datos que contiene, hasta que se pague un rescate al atacante. Por lo general, el Ransomware se propaga a través de correos electrónicos de phishing o mediante descargas de software infectado.
- Phishing: Se usa mucho en la ciberdelincuencia con la finalidad de timar a cada persona y tener informaciones confidenciales, sean una contraseña, número de tarjeta de crédito o informaciones de tipo financiero. Cada atacante suele hacerse pasar por empresas o entidades legítimas para engañar a las personas y obtener información.
- Spoofing: Es una técnica de falsificación utilizada para engañar a las personas o a los sistemas informáticos, haciéndoles creer que la información que están recibiendo es legítima y confiable. Por ejemplo, el Spoofing de direcciones de correo electrónico es común en los ataques de phishing, donde los atacantes falsifican la dirección del remitente para que parezca que proviene de una fuente legítima.
- Ataques de falsificación: También conocidos como ataques de presentación, se refieren al uso de copias falsificadas de los rasgos biométricos de un individuo para engañar al sistema de autenticación. Esto puede hacerse mediante la

impresión de una imagen de alta calidad de la huella dactilar o mediante la creación de una máscara facial para burlar el reconocimiento facial.

- Ataques de suplantación: Estos ataques implican la creación de una identidad falsa utilizando los datos biométricos de otra persona. Por ejemplo, un atacante podría intentar utilizar la huella dactilar de una persona para hacerse pasar por ella y acceder a sistemas protegidos por biometría.
- Ataques de ingeniería social: En estos ataques, los atacantes manipulan a los usuarios para que proporcionen sus datos biométricos de forma voluntaria o involuntaria. Por ejemplo, un atacante podría hacerse pasar por un representante del servicio técnico y pedir a los usuarios que proporcionen su huella dactilar para solucionar un problema.
- Ataques de interceptación: Estos ataques implican la interceptación de los datos biométricos durante la transmisión entre el sensor y el sistema de autenticación. Un atacante podría interceptar los datos de reconocimiento facial o de huellas dactilares para acceder a sistemas protegidos.
- Ataques de robo de credenciales: Aunque no se trata específicamente de un ataque biométrico, los atacantes pueden intentar robar las credenciales de autenticación biométrica de un usuario para acceder a sistemas protegidos. Esto podría hacerse mediante la interceptación de contraseñas o mediante el secuestro de credenciales biométricas almacenadas en el dispositivo del usuario.
- App: (Application software). Hace referencia a la abreviatura de aplicación informática, ella está definida como programa de informática cuyo diseño busca brindar ayuda a los usuarios para que realicen una tarea específica. Asimismo, cada aplicación puede ser estándar o desarrollarse a medida con la finalidad de lograr la cobertura de cada necesidad particular de cada usuario en concreto.
- Cloud Computing: Es un innovador enfoque tecnológico donde las aplicaciones de software y los recursos de hardware, incluyendo la capacidad de procesamiento y almacenamiento de datos, no residen en los dispositivos del usuario, sino en un centro de datos remoto. Esto permite a los usuarios acceder

fácilmente a aplicaciones y servicios a través de Internet, comúnmente referido como 'la Nube', de manera conveniente y sencilla.

- Active Directory. Es un servicio de directorio que gestiona la autenticación de usuarios y controla el acceso a una variedad de recursos, como computadoras personales, servidores, sistemas de almacenamiento y aplicaciones.

Referencias

Amjad, M. &, Ayman, M. (2021). Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing. *Tech Science Press - Computer Systems Science & Engineering*, *43*(3), 967-984. DOI: 10.32604/csse.2022.024854

Balbix. *What is the NIST Cybersecurity Framework?*. Recuperado el 15 de marzo de 2023, de https://www.balbix.com/insights/nist-cybersecurity-framework/.

Bader, A., Muhammad, H., Alharbi, A., Wael, A., Alyami, H., &, Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategieset. *IEEE Access, 9,* 57792-57807. DOI: 10.1109/ACCESS.2021.3073203. https://ieeexplore.ieee.org/document/9404177

Banger, N., Pallavi, K., & Shetty, S. J. (2022). A Review Paper on Cloud Computing Architecture Types Advantages and Disadvantages. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 2*(2), 14-22. https://ijarsct.co.in/Paper3144.pdf

Chatterjee, S., Peffers, K., Tuunanen, T., & Rothenberger, M., (2007). Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45-77. DOI: 10.2753/MIS0742-1222240302

Cortés Osorio, J. A., Medina Aguirre, F. A., & Muriel Escobar, J. A. (2010). *Sistemas de seguridad basados en Biometría*. *Scientia et technica, 17*(46), 98-102. https://www.redalyc.org/pdf/849/84920977016.pdf

De la Vega M. F., Robles, R. D., Garcia, B. A., Flores, P., Hernandez D., & Garcia, A. (2020, 24-26 de agosto). *Diseño conceptual de un sistema biométrico para casilleros* [Conferencia]. CASE, Argentina.

https://www.researchgate.net/publication/356541835_Diseno_conceptual_de_un_sistema_biometrico_para_casilleros

ESET. (2022). *Principales preocupaciones de las empresas en América Latina en temas de seguridad*. ESET https://www.welivesecurity.com/wp-content/uploads/2022/07/ESET-security-report-LATAM-2022.pdf.

ESGINNOVA Group. (2019, 22 de agosto). ISO 27001. *Aspectos claves y relación con las normas ISO 22301 e ISO/IEC 20000*. Recuperado el 15 de marzo de 2023, de https://www.pmg-ssi.com/2019/08/iso-27001-aspectos-claves-y-relacion-con-las-normas-iso-22301-e-iso-iec-20000/.

IBM. (2022). Top attacked industries. https://www.ibm.com/downloads/cas/ADLMYLAZ.

Irshad, A., Chaudhry, S. A., Alomari, O. A., Yahya, K., & Kumar, N. (2020). A novel pairing-free lightweight authentication protocol for mobile cloud computing framework. *IEEE Systems Journal*, *15*(3), 3664-3672.

ISO Tools. (2023). *ISO/IEC 27002:2022 Controles Organizacionales. Todo lo que necesita saber*. Recuperado el 25 de abril de 2023, de https://www.isotools.us/2022/07/29/iso-iec-270022022-controles-organizacionales-todo-lo-que-necesitas-saber/.

Organización Internacional de Normalización. (2023). ISO/IEC 27002:2013. 14 dominios, 35 objetivos de control y 114 controles. Recuperado el 25 de abril de 2023, de https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf.

Kanak, A. (2018). Biometric ontology for semantic biometric-asa-service (BaaS) applications: a border security use case. *IET Biometrics, 7*(6), 510-518. https://doi.org/10.1049/iet-bmt.2018.5067

Kang, T. K. (2022). Emotion Recognition using Short-Term Multi-Physiological Signals. *KSII Transactions on Internet & Information Systems, 16*(3). http://doi.org/10.3837/tiis.2022.03.018

Kolhar, M., Al-Turjman, F., Alameen, & A., Abualhaj, M. (2020). A three layered decentralized IoT biometric architecture for city lockdown during COVID-19 outbreak. *IEEE Access, 8,* 163608-163617. https://doi.org/10.1109/ACCESS.2020.3021983

Kumar, P., Seth, S., Bajaj, K., & Rawat, S. (2019, noviembre 22-23). *Diverse security practices and comparison on key stroke dynamics* [Conferencia]. 8th International Conference System Modeling and Advancement in Research Trends, Moradabad, India. https://ieeexplore.ieee.org/abstract/document/9117401

Congreso de la República del Perú (2013). *Ley N.° 29733 de 2013. Por lo cual se expide Ley de Protección de Datos Personales*. https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf

Congreso de la República del Perú (2000). *Ley N.° 27269 de 2000. Por lo cual se expide Ley de Firmas y Certificados Digitales y su Reglamento.* https://diariooficial.elperuano.pe/pdf/0030/ley-27269.pdf.

Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Ariffin, S. A. B., Alemran, A., ... & Garfan, S. (2020). Finger vein biometrics: taxonomy analysis, open challenges, future directions, and recommended solution for decentralised network architectures. *IEEE Access, 8*, 9821-9845.

Mudhhi, F., Mohamed, A. &, Ouda, O. (2022). A secure identity and access management framework in cloud environment based on dual-factor authentication. *Journal of Theoretical and Applied Information Technology, 100* (3). https://www.jatit.org/volumes/Vol100No3/8Vol100No3.pdf

Nakanishi, I., & Maruoka, T. (2019). Biometrics using electroencephalograms stimulated by personal ultrasound and multidimensional nonlinear features. *Electronics, 9*(1), 24. DOI: 10.3390/electronics9010024.

Stafford, V. A. (2020). Zero trust architecture. *NIST special publication, 800*, 207. https://doi.org/10.6028/NIST.SP.800-207

Olukoya, O. (2022). Assessing frameworks for eliciting privacy & security requirements from laws and regulations. *Computers & Security,* 117 (2022). https://doi.org/10.1016/j.cose.2022.102697

Osorio-Roig, D., Rathgeb, C., Drozdowski, P., & Busch, C. (2021). Stable hash generation for efficient privacy-preserving face identification. *IEEE Transactions on Biometrics, Behavior, and Identity Science, 4*(3), 333-348. https://doi.org/10.1109/TBIOM.2021.3100639

Rui, Z., & Yan, Z. (2018). A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE access, 7*, 5994-6009. https://doi.org/10.1109/ACCESS.2018.2889996

Jangid, P. S., & Bharadi, V. A. (2020, febrero 18-20). *Evolving Authentication Design Consideration and BaaS Architecture for Internet of Biometric things* [Conferencia]. International Conference on Convergence to Digital World-Quo Vadis (ICCDW), Mumbai, India. https://doi.org/10.1109/ICCDW45521.2020.9318664

Saqib, N. U., Arora, M., & Chopra, S. (2018). Cloud Computing Architecture Issues and Future Research Directions. *International Journal of Emerging Technologies and Innovative Research*, *5*(11), 532-537. http://www.jetir.org/papers/JETIRDR06081.pdf

Sarkar, A., &, Singh, B. (2020). A review on performance, security, and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications 79*(37-38), 27721-27776. DOI: 10.1007/s11042-020-09197-7

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. JOIV: *International Journal on Informatics Visualization, 4*(4), 225-230. https://joiv.org/index.php/joiv/article/view/482

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE Access, 10*, 57143-57179. https://doi.org/10.1109/ACCESS.2022.3174679

Tian, H., Li, X., Quan, H., Chang, C., & Baker, T. (2021). A Lightweight Attribute-Based Access Control Scheme for Intelligent Transportation System with Full Privacy Protection. *IEEE Sensors Journal*, *21*(14), 15793-15806. DOI: 10.1109/JSEN.2020.3030688

Walsh, K., & Manferdelli, J. (2017, junio 25-30). *Intra-cloud and inter-cloud authentication* [Conferencia]. IEEE 10th International Conference on Cloud Computing (CLOUD), Honololu, USA. https://doi.org/10.1109/CLOUD.2017.48

Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: *Approaches, threats and trends. Computer Networks*. DOI: 170,107118. 10.1016/j.comnet.2020.107118

Wortman, P., Yan, W., Chandy, J., & Tehranipoor, F. (2018). P2M-based security model: security enhancement using combined PUF and PRNG models for authenticating consumer electronic devices. *IET Computers & Digital Techniques, 12*(6), 289-296. https://doi.org/10.1049/iet-cdt.2018.5099

Yamada, A., & Ikeda, T. (2017). Enhanced PKI authentication with trusted product at claimant. *Computers & Security, 67*, 324-334. https://doi.org/10.1016/j.cose.2017.01.001

Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for internet-of-things security: A review. *Sensors, 21*(18), 1-26. https://doi.org/10.3390/s21186163

Anexos

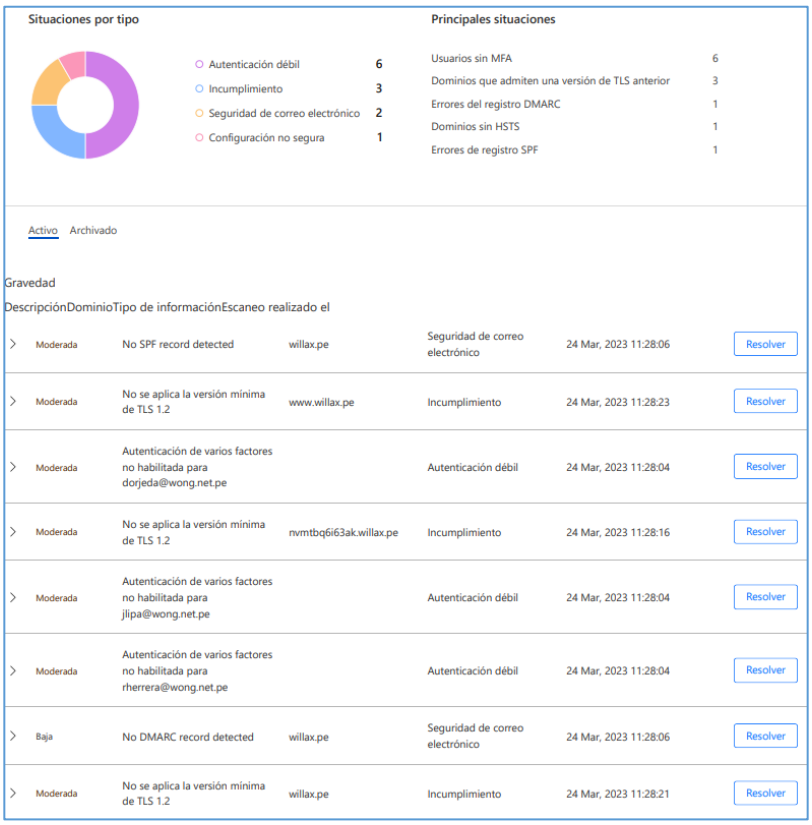
Anexo 1.
Implementación de la solución propuesta

Para la prueba de la solución propuesta, el escenario que elegimos fue la nube de Google (GCP) donde implementamos la autenticación biométrica a los recursos (instancias) con IAM (identity Access management) y el API Identity Aware Proxy que intercepta las solicitudes web recibidas; utilizamos el servicio de identidad de Google y solo se permitió el acceso a usuarios autorizados.

Por otro lado, mostramos un reporte de la herramienta Cloudflare para una página web alojada en la nube de una empresa retail. Cloudflare es una plataforma global en la nube diseñada para que todos los recursos conectados a internet sean seguros, privados, rápidos y fiables. que se cual controla las vulnerabilidades en la nube.

Figura 24

Reporte de vulnerabilidades



Situaciones por tipo

Autenticación débil	6
Incumplimiento	3
Seguridad de correo electrónico	2
Configuración no segura	1

Principales situaciones

Usuarios sin MFA	6
Dominios que admiten una versión de TLS anterior	3
Errores del registro DMARC	1
Dominios sin HSTS	1
Errores de registro SPF	1

Activo Archivado

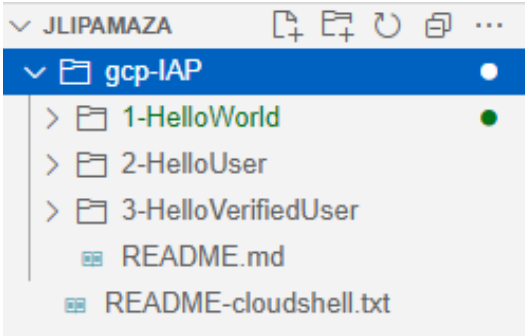
Gravedad	Descripción	Dominio	Tipo de información	Escaneo realizado el	
Moderada	No SPF record detected	willax.pe	Seguridad de correo electrónico	24 Mar, 2023 11:28:06	Resolver
Moderada	No se aplica la versión mínima de TLS 1.2	www.willax.pe	Incumplimiento	24 Mar, 2023 11:28:23	Resolver
Moderada	Autenticación de varios factores no habilitada para dorjeda@wong.net.pe		Autenticación débil	24 Mar, 2023 11:28:04	Resolver
Moderada	No se aplica la versión mínima de TLS 1.2	nvmtbq6i63ak.willax.pe	Incumplimiento	24 Mar, 2023 11:28:16	Resolver
Moderada	Autenticación de varios factores no habilitada para jlipa@wong.net.pe		Autenticación débil	24 Mar, 2023 11:28:04	Resolver
Moderada	Autenticación de varios factores no habilitada para rherrera@wong.net.pe		Autenticación débil	24 Mar, 2023 11:28:04	Resolver
Baja	No DMARC record detected	willax.pe	Seguridad de correo electrónico	24 Mar, 2023 11:28:06	Resolver
Moderada	No se aplica la versión mínima de TLS 1.2	willax.pe	Incumplimiento	24 Mar, 2023 11:28:21	Resolver

Este reporte muestra muchas vulnerabilidades asociadas a la autenticación. Esto es una gran premisa para impulsar el uso de la solución propuesta.

1. Primero realizamos la prueba con una página web hecha en Python previamente cargada a la consola de Google.

Figura 25

Página web en plataforma Google Cloud



2. Luego desplegaremos la página en el proyecto para tenerla como una instancia y seguidamente la habilitaremos para su navegación.

Figura 26

Instancia de la página web

3. Una vez realizada la habilitación se puede acceder a la página previamente subida

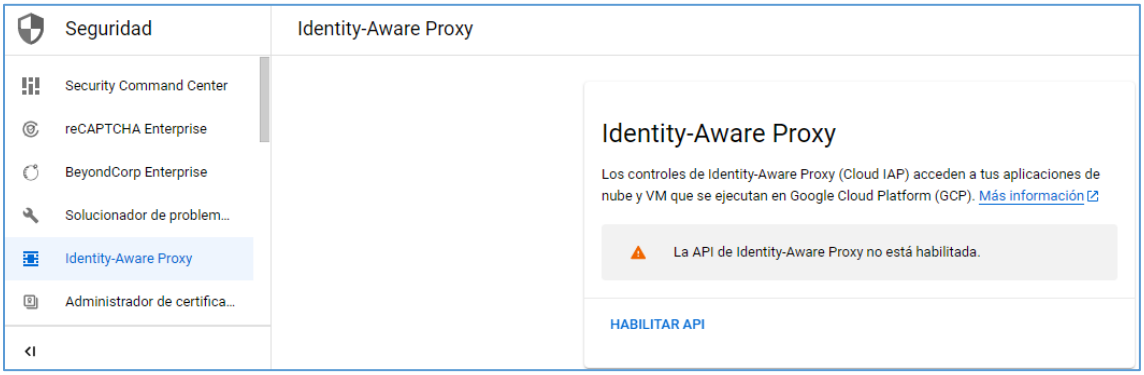
Figura 27

Acceso a la página web

4. Este acceso es sin ningún tipo de autenticación. Después de esto instalaremos el API Identity Aware Proxy dentro de la consola de Google.

Figura 28

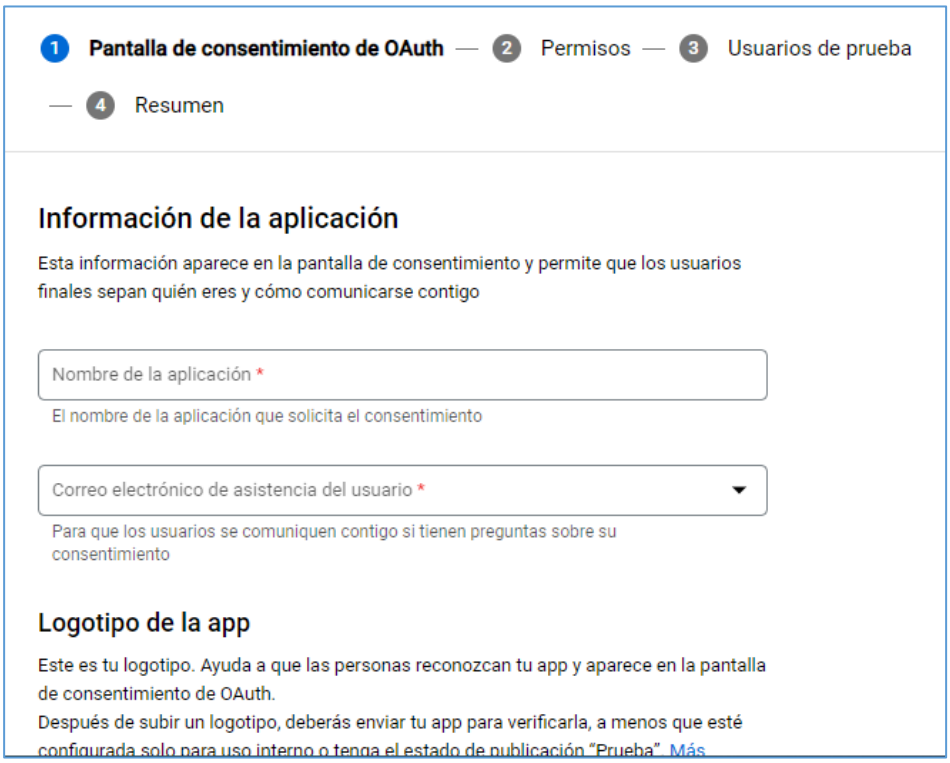
API Identity Aware Proxy



5. Luego aprobaremos el consentimiento de uso del protocolo Oauth y seguidamente completaremos el formulario con información de la página previamente cargada.

Figura 29

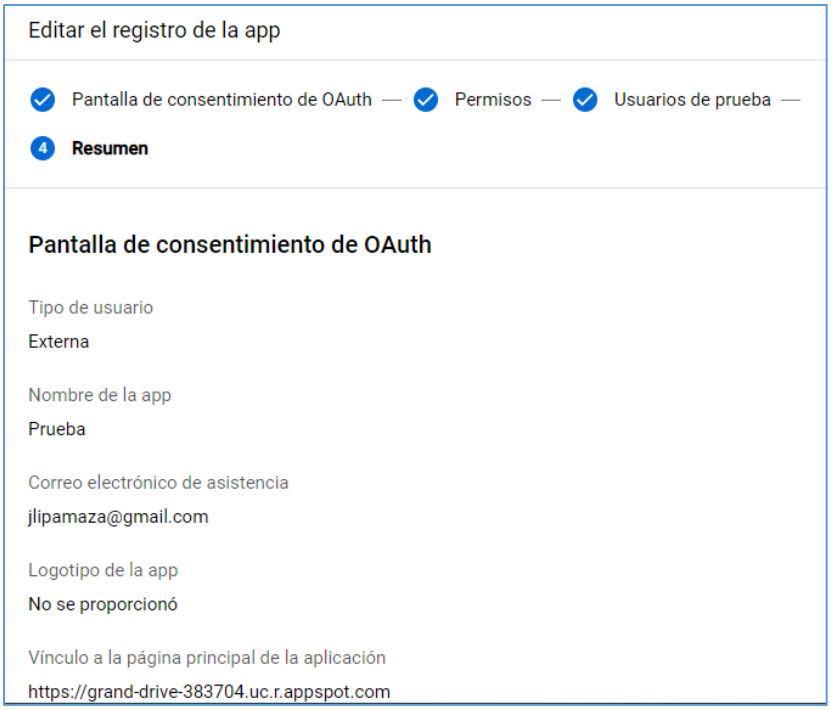
Uso del protocolo Oauth



6. Una vez completada la configuración de consentimiento de uso del protocolo Oauth a nuestra página, procederemos a ir a la configuración del uso del API.

Figura 30

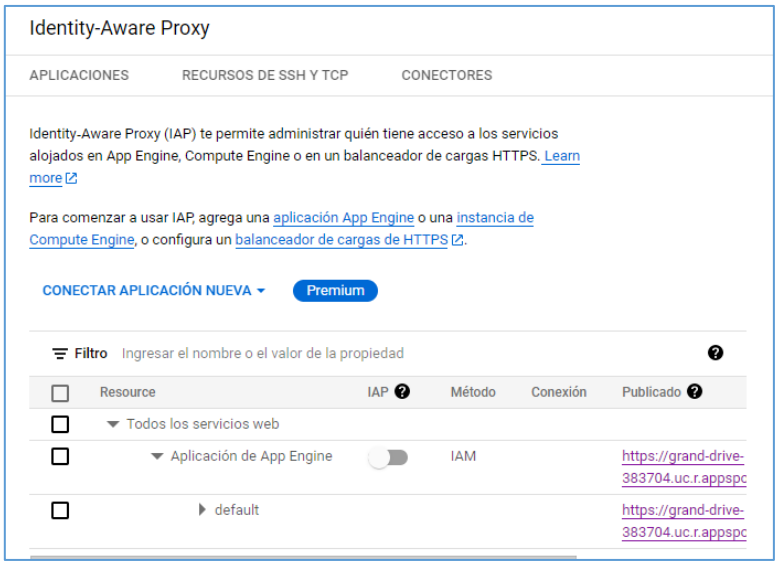
Configuración del uso del API



7. Aquí habilitaremos el API para el uso en APP Engine.

Figura 31

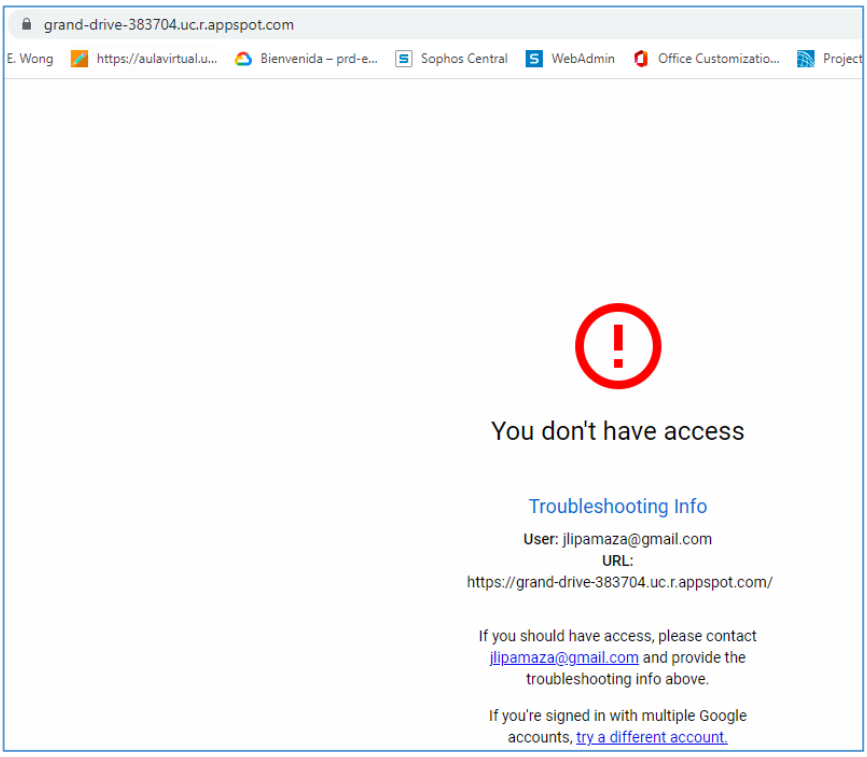
Habilitar el API para el uso en APP Engine



8. Seguidamente volveremos a probar el acceso a nuestra página.

Figura 32

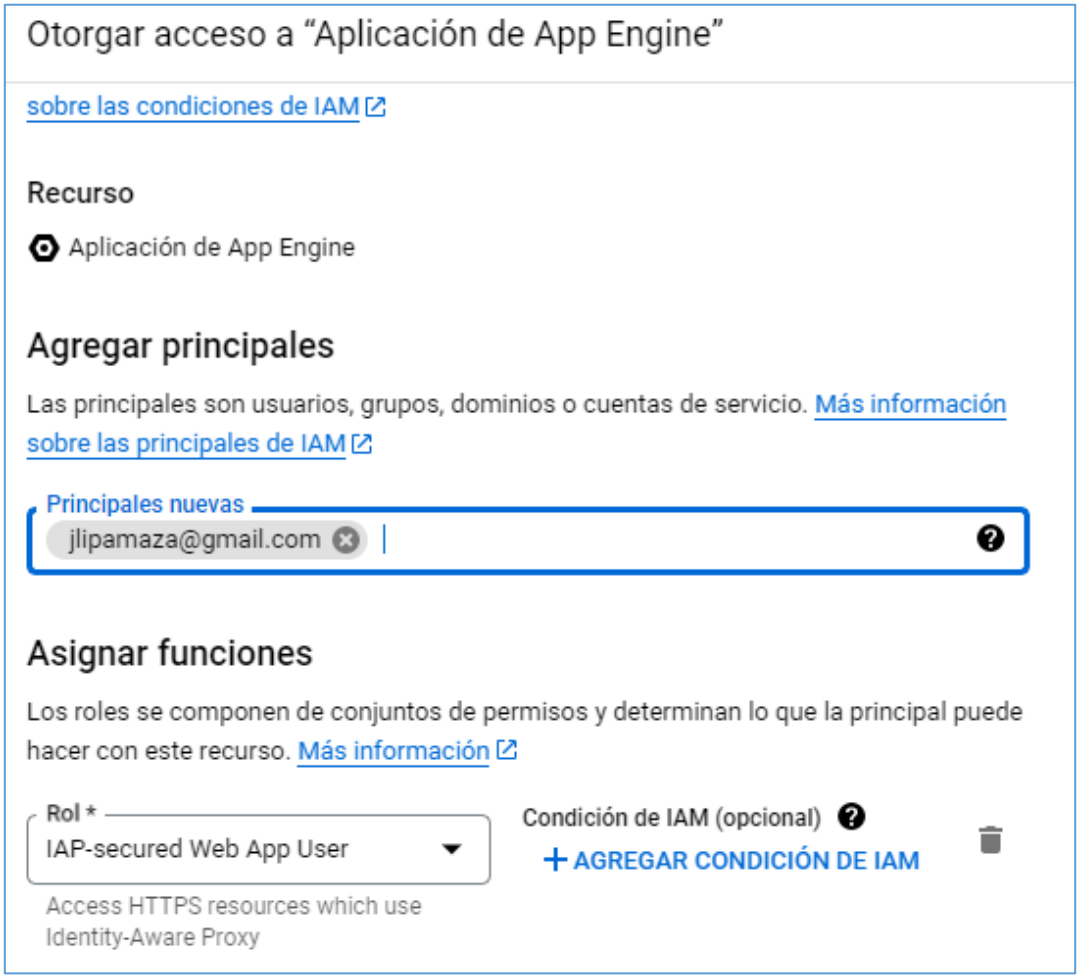
Prueba de acceso a la página web



9. Vemos que la autenticación no permite acceder al usuario previamente autenticado, ya que aún no se ha agregado a ninguno. Entonces ahora procederemos a agregarlo como parte del servicio IAM como parte de una autorización a un recurso.

Figura 33

Autenticación no permita

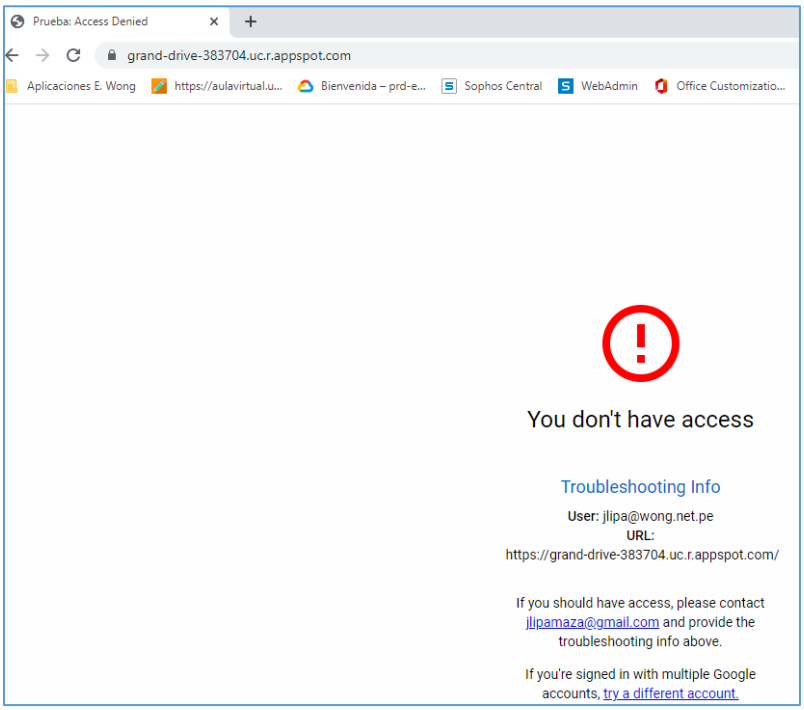


10. Este permiso permite al usuario independiente de si está como parte del proyecto o no poder hacer uso del API para poder autenticarse y luego acceder al recurso. Una vez agregado el usuario, para nuestro ejemplo es jlipamaza@gmail.com, volveremos a intentar acceder con un usuario diferente y luego con el usuario autorizado.

Usuario distinto:

Figura 34

Autenticación no permita



Usuario autorizado: Para el uso de la biometría se asociará la cuenta de correo a una aplicación de autenticación, en este caso Microsoft authenticator, que está previamente asociado al registro biométrico en el equipo celular.

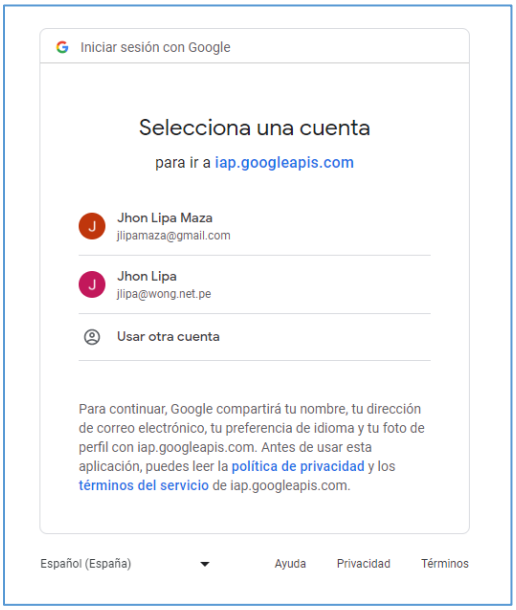
Figura 35

Software Microsoft Authenticator

Primero, elegiremos la cuenta asociada, jlipamaza@gmail.com para nuestro caso.

Figura 36

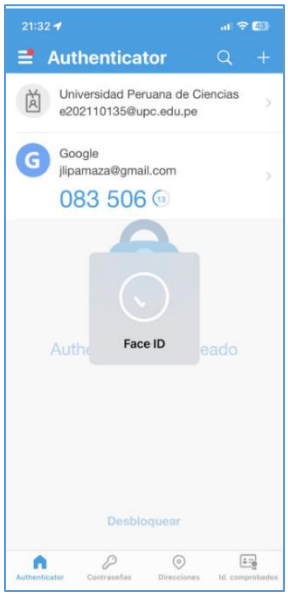
Selección de cuenta de correo



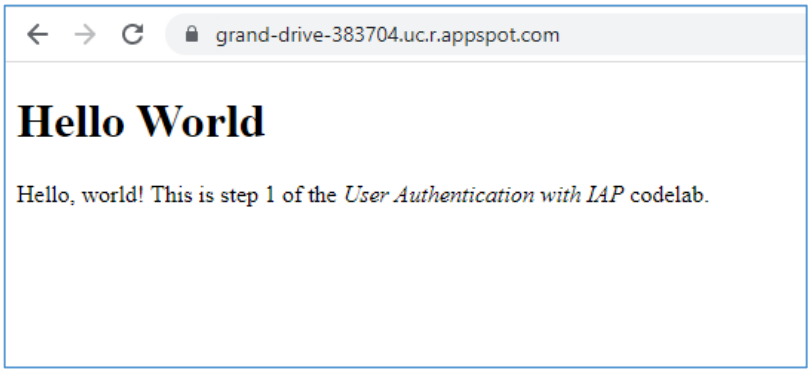
Cuando el usuario intenta ingresar a la página web, la aplicación lanza una solicitud de aprobación de identidad.

Figura 37

Software Microsoft Authenticator



Y, finalmente, se verá el ingreso al sitio web exitoso.

Figura 38

Ventana de bienvenida después de la autenticación satisfactoria