

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE



“DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE
GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESO PARA
PYMEs BASADA EN SERVICIOS CLOUD”

ALEJANDRO IGNACIO CUBILLOS HIDALGO

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA

Profesor Guía: Raúl Monge Anwandter

Profesor Correferente: Raquel Pezoa

Octubre - 2026

CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Título del trabajo: Diseño e implementación de una solución de gestión de identidades y control de acceso para pymes basada en servicios cloud

Nombre del candidato(a): Alejandro Ignacio Cubillos Hidalgo

Carrera / Grado: Ingeniería Civil Informática

Campus: Casa Central Departamento: Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Raúl Monge Anwandter, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

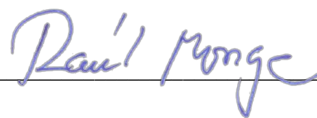
Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 24 sept. 2026

Firma:



Estudiante o Candidato(a):

Fecha: 23/09/2026

Firma:



Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

DEDICATORIA

Esta Tesis se la quiero dedicar a mi familia que siempre estuvieron acompañándome en este importante proceso.

AGRADECIMIENTOS

En primer lugar, quiero expresar mi más sincero agradecimiento a mis padres, quienes me brindaron un apoyo incondicional desde que inicié esta etapa universitaria. Siempre estuvieron presentes cuando más los necesité, a pesar de las pruebas y dificultades que se me presentaban en la vida. También agradezco a mi tía y a mi hermana, quienes estuvieron a mi lado en mis momentos de mayor debilidad, ayudándome a aprender a cómo perseverar en esta travesía.

Quiero dar las gracias a mis compañeros y a todas las personas que conocí y me ayudaron durante estos años en la universidad. Ellos me brindaron su apoyo y conocimientos, compartimos largas jornadas de trabajo y momentos de esparcimiento que hicieron este camino más llevadero.

Finalmente, quiero expresar mi más profunda gratitud a mi profesor guía Raul Monge, quien me acompañó de manera ejemplar en todo este proceso. Me guio, aconsejó y brindó su valiosa mentoría a través del desarrollo de esta memoria.

RESUMEN

Resumen— Las Pequeñas y Medianas Empresas (PYMEs) enfrentan importantes desafíos en ciberseguridad debido al uso de mecanismos tradicionales de autenticación y control de acceso, los cuales suelen presentar debilidades de seguridad y dificultades de administración. Además, las leyes chilenas 21.719 y 21.663 exigen medidas adecuadas para proteger la información y gestionar el acceso a los sistemas.

Este trabajo propone y evalúa el diseño de una solución de gestión de identidades y control de acceso para PYMEs, basada en autenticación centralizada, control de acceso basado en roles (RBAC) y servicios *cloud*. Para ello, se desarrolló un prototipo funcional utilizando la plataforma Base44, incorporando gestión de usuarios, autenticación integrada y APIs protegidas.

La validación del prototipo permitió comprobar que este enfoque mejora la administración de accesos, restringe funcionalidades según el rol del usuario y fortalece la seguridad de los recursos protegidos, representando una alternativa viable y de bajo costo para PYMEs.

Palabras Clave— Control de acceso, PYMEs, Gestión de identidades, RBAC, Ciberseguridad, APIs protegidas, Servicios *cloud*.

ABSTRACT

Abstract— Small and medium-sized enterprises (SMEs) face significant cybersecurity challenges due to their use of traditional authentication and access control mechanisms, which often exhibit security weaknesses and management difficulties. Furthermore, Chilean laws 21.719 and 21.663 mandate appropriate measures to protect information and manage access to systems.

This work proposes and evaluates the design of an identity management and access control solution for SMEs, based on centralized authentication, role-based access control (RBAC), and cloud services. To this end, a functional prototype was developed using the Base44 platform, incorporating user management, integrated authentication, and protected APIs.

Validation of the prototype confirmed that this approach improves access management, restricts functionalities based on user roles, and strengthens the security of protected resources, representing a viable and low-cost alternative for SMEs.

Keywords— Access control, SMEs, Identity management, RBAC, Cybersecurity, Secure APIs, Cloud services.

INDICE DE CONTENIDOS

DEDICATORIA	3
AGRADECIMIENTOS.....	4
RESUMEN	5
ABSTRACT	5
INDICE DE CONTENIDOS	6
CAPÍTULO 1: INTRODUCCIÓN.....	9
1.1 Definición del problema	9
1.1.1 Contexto del problema.....	10
1.1.2 Especificación del problema.....	11
1.2 Objetivos.....	13
1.2.1 Objetivo general	13
1.2.2 Objetivos específicos.....	13
1.3 Organización del documento.....	14
CAPÍTULO 2: MARCO CONCEPTUAL.....	15
2.1 Sistemas de control de acceso	15
2.1.1 Identificación.....	15
2.1.2 Autenticación	16
2.1.3 Autorización	16
2.1.4 Modelos de control de acceso	17
2.2 Evolución de los Mecanismos de Autenticación y Autorización.....	21
2.2.1 Autenticación Tradicional Basada en Credenciales.....	21
2.2.2 Autenticación Basada en Sesiones e Inconvenientes en Arquitecturas Modernas.....	21
2.2.3 Autenticación Desacoplada mediante Tokens de Identidad (JWT)	22
2.2.4 De la Autenticación Local a la Autorización Delegada y Federación	22
2.2.5 Comparativa de la Evolución Tecnológica de Control de Acceso	23
2.3 OAuth 2.0 como base para autenticación y autorización moderna	23
2.3.1 Componentes principales.....	24
2.3.2 Flujos de autorización	25
2.4. OpenID Connect (OIDC)	26
2.5. Inicio de sesión único (SSO)	28
2.6. Plataformas Cloud de Desarrollo y Servicios de Autenticación Integrada (SaaS/BaaS)	28
2.7. Gestión de Identidades y Accesos (IAM)	29
2.8. Contexto de aplicación en PYMEs	29

2.9.	Arquitectura conceptual de gestión de identidades y control de acceso	30
2.10.	Marco normativo aplicable a la gestión de identidades y accesos en PYMEs en Chile	31
2.11.	Síntesis del marco conceptual	33
CAPÍTULO 3: PROPUESTA DE SOLUCIÓN		34
3.1	Diagnóstico	35
3.2	Análisis.....	35
3.3	Diseño de la solución.....	36
3.3.1	Caso de estudio: Modelo organizacional y roles de la PYME "Dulce Aroma"	37
3.3.2	Principios de diseño	38
3.3.3	Arquitectura propuesta.....	38
3.3.4	Flujo de autenticación	39
3.4	Tecnologías y herramientas empleadas en la implementación del prototipo	40
3.5	Implementación	42
3.6	Despliegue	43
3.7	Beneficios de la solución	43
3.8	Evaluación económica y estimación de esfuerzo.....	44
3.9	Síntesis de la propuesta.....	44
CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN Y PRUEBAS DEL PROTOTIPO		46
4.1	Descripción general del prototipo implementado.....	46
4.2	Implementación del prototipo.....	46
4.3	Pruebas realizadas sobre el prototipo	47
4.4	Resultados obtenidos.....	48
4.4.1	Resultado de la prueba 1: Registro de usuarios	48
4.4.2	Resultado de la prueba 2: Inicio de sesión válido	50
4.4.3	Resultado de la prueba 3: Restricción de acceso a usuarios no autenticados	53
4.4.4	Resultado de la prueba 4: Control de acceso basado en roles.....	54
4.4.5	Resultado de la prueba 5: Inactividad de sesión (Time-out)	57
4.5	Seguridad en el acceso a la aplicación Web	58
4.6	Continuidad operativa y resiliencia	59
4.7	Consideraciones sobre autenticación entre servicios	59
CAPÍTULO 5: CONCLUSIONES		60
5.1	Cumplimiento de los objetivos	60
5.2	Principales aportes del trabajo	61

5.3	Limitaciones del trabajo	61
5.4	Trabajo futuro	62
REFERENCIAS BIBLIOGRÁFICAS		63

CAPÍTULO 1: INTRODUCCIÓN

En la actualidad, la transformación digital ha impulsado a las Pequeñas y Medianas Empresas (PYMEs) a adoptar sistemas informáticos y servicios digitales para gestionar sus operaciones críticas. Sin embargo, este avance tecnológico no siempre ha sido acompañado por mecanismos adecuados de seguridad y control de acceso. Muchas PYMEs continúan utilizando esquemas tradicionales de autenticación basados únicamente en usuarios y contraseñas administradas localmente, lo que incrementa el riesgo de accesos no autorizados, filtraciones de información y vulnerabilidades asociadas al manejo inseguro de credenciales.

Esta situación adquiere mayor relevancia en el contexto chileno actual, donde la Ley 21.719 de Protección de Datos Personales y la Ley 21.663 Marco de Ciberseguridad establecen la necesidad de implementar medidas adecuadas para proteger la información y garantizar una gestión segura del acceso a los sistemas. El incumplimiento de estas normativas puede generar sanciones legales, afectar la continuidad operativa y comprometer la confianza de clientes y socios comerciales.

El desafío para las PYMEs radica en implementar soluciones de autenticación y control de acceso que sean seguras, escalables y compatibles con sus limitaciones de presupuesto y personal técnico especializado. En este contexto, los mecanismos modernos de autenticación centralizada, gestión de identidades y control de acceso basado en roles (RBAC) surgen como alternativas que permiten mejorar la seguridad sin requerir una infraestructura compleja administrada localmente.

Este trabajo de título propone el diseño e implementación de una solución de gestión de identidades y control de acceso orientada a PYMEs, utilizando servicios *cloud* para centralizar la autenticación, administración de usuarios y protección de recursos. Para ello, se desarrolló un prototipo funcional utilizando la plataforma Base44, incorporando mecanismos de autenticación integrada, control de acceso basado en roles y APIs protegidas. A través de la implementación y validación del prototipo, esta investigación busca demostrar que es posible fortalecer la postura de ciberseguridad de una PYME mediante soluciones modernas, accesibles y de bajo costo.

1.1 Definición del problema

En la actualidad, las pequeñas y medianas empresas (PYMEs) enfrentan un entorno digital cada vez más complejo, donde la seguridad de la información se ha convertido en un aspecto crítico para la continuidad operativa y la protección de los datos. Sin embargo, muchas de estas organizaciones carecen de mecanismos adecuados para gestionar el acceso a sus sistemas, lo que las expone a riesgos como accesos no autorizados, filtraciones de información y uso indebido de credenciales.

A diferencia de las grandes organizaciones, que cuentan con infraestructura robusta y equipos especializados en ciberseguridad, las PYMEs presentan limitaciones en términos de recursos económicos, capacidades técnicas y conocimiento especializado. Esto dificulta la implementación de soluciones modernas de autenticación, gestión de identidades y control de acceso.

En este contexto, la ausencia de mecanismos centralizados de autenticación y autorización representa una brecha significativa en la seguridad de estas organizaciones. Muchas PYMEs continúan utilizando esquemas tradicionales basados únicamente en usuario y contraseña, sin políticas adecuadas de control de acceso ni mecanismos seguros para la administración de identidades, aumentando así la superficie de ataque y el riesgo de incidentes de seguridad.

1.1.1 Contexto del problema

La transformación digital ha dejado de ser una opción para convertirse en un requisito fundamental para la continuidad operativa de las organizaciones modernas, incluyendo a las PYMEs. La adopción de plataformas web, servicios *cloud* y herramientas digitales ha permitido optimizar procesos y mejorar la conectividad, pero también ha incrementado significativamente la superficie de ataque y la exposición a incidentes de ciberseguridad.

A diferencia de las grandes corporaciones, las PYMEs suelen operar con presupuestos limitados y una reducida disponibilidad de personal especializado en seguridad informática. Como consecuencia, muchas organizaciones continúan utilizando mecanismos tradicionales de autenticación basados únicamente en usuario y contraseña, administrados de forma local y sin controles centralizados adecuados. Esta situación favorece prácticas inseguras, como el uso de contraseñas débiles, la reutilización de credenciales y la ausencia de políticas formales de administración de accesos.

La relevancia de esta problemática se ve reforzada por el actual marco regulatorio chileno. La Ley N° 21.719 de Protección de Datos Personales y la Ley N° 21.663 Marco de Ciberseguridad establecen la necesidad de implementar medidas adecuadas para proteger la información sensible y asegurar el acceso a los sistemas. El incumplimiento de estas normativas puede generar sanciones legales, afectar la continuidad operativa y comprometer la confianza de clientes y socios comerciales.

Diversos estudios reflejan el impacto de estas vulnerabilidades en organizaciones de menor tamaño:

- Según reportes de Verizon, aproximadamente el 43% de las brechas de datos afectan a pequeñas empresas, debido principalmente a la falta de controles de seguridad adecuados [1].
- El uso de credenciales comprometidas o débiles continúa siendo una de las principales causas de incidentes de seguridad e intrusiones exitosas en sistemas corporativos.
- En el contexto de las PYMEs, factores como la limitada alfabetización digital, configuraciones inseguras y la ausencia de políticas de seguridad incrementan la exposición a amenazas cibernéticas.

Frente a este escenario, los mecanismos modernos de autenticación centralizada, gestión de identidades y control de acceso basado en roles (RBAC) permiten fortalecer la seguridad y simplificar la administración de usuarios. Asimismo, el uso de plataformas y servicios cloud facilita la adopción de estas tecnologías sin requerir infraestructura compleja ni altos costos

operativos, lo que las convierte en una alternativa especialmente adecuada para organizaciones con recursos técnicos y económicos limitados.

En este contexto, mejorar los mecanismos de control de acceso en las PYMEs resulta fundamental para reducir la exposición a amenazas de seguridad, proteger la información de la organización y de sus clientes, y disminuir los riesgos asociados al uso inseguro de credenciales. Además, la adopción de soluciones de autenticación centralizada contribuye al cumplimiento de la normativa chilena vigente en materia de protección de datos personales y ciberseguridad, fortaleciendo la postura de seguridad de las organizaciones y facilitando la administración de accesos.

En consecuencia, el desafío de esta investigación consiste en proponer una solución de control de acceso que sea segura, escalable y viable para el entorno de las PYMEs chilenas, considerando sus limitaciones técnicas y económicas, así como las exigencias actuales en materia de protección de datos y ciberseguridad.

1.1.2 Especificación del problema

Lo anterior conduce a formular una definición más precisa del problema abordado en esta memoria:

- ¿De qué manera diseñar e implementar una solución de control de acceso basada en mecanismos modernos de autenticación centralizada, autorización y gestión de identidades, que sea segura, adaptable a las limitaciones técnicas de las PYMEs en Chile y que permita cumplir con el marco regulatorio vigente mediante el uso de servicios *cloud*?

Dado este contexto, es posible identificar los principales *stakeholders* involucrados en el problema, los cuales se verán afectados directa o indirectamente por la implementación de la solución propuesta. La Tabla 1 presenta el detalle de estos actores:

- **Dueños y Administradores de PYMEs:** Responsables legales y de la toma de decisiones estratégicas. Requieren garantizar la continuidad operativa, mitigar riesgos de ciberseguridad y evitar sanciones por incumplimiento normativo (Leyes 21.719 y 21.663).
- **Empleados de la organización (Usuarios finales):** Personal administrativo y operativo que accede a las herramientas del sistema. Requieren mecanismos de acceso simples y seguros que no entorpezcan su labor diaria.
- **Personal técnico o desarrolladores internos:** Encargados de la mantención e integración de las soluciones tecnológicas. Requieren arquitecturas de baja complejidad de administración
- **Clientes de la PYME:** *Stakeholders* clave del negocio cuya información personal y transaccional es procesada por la empresa. Dependen de que la PYME implemente controles de acceso adecuados para garantizar la confidencialidad de sus datos y cumplir con la Ley N° 21.719.

Es importante aclarar que, si bien los clientes representan un *stakeholder* clave en el modelo de negocio y en la protección de datos personales de la PYME, el alcance del prototipo desarrollado en este trabajo se enfoca en el control de acceso y gestión de identidades para las interfaces y roles internos de la organización.

Asimismo, existen otros actores relevantes que, si bien no participan directamente en la implementación técnica, se ven impactados por la seguridad del sistema y la gestión de la información:

- **Organismos reguladores y fiscalizadores** (Agencia de Protección de Datos): Entidades que velan por el cumplimiento del marco legal de ciberseguridad y protección de datos en Chile.
- **Proveedores de Servicios Cloud y Plataformas de Identidad**: Entidades externas que suministran la infraestructura tecnológica y los servicios gestionados de autenticación.

A continuación, se presenta el detalle de los actores principales en la tabla 1:

Tabla 1: Stakeholders del Problema.

Stakeholder	Descripción	Relación
Dueños y Administradores	Representantes legales y responsables de la toma de decisiones en la PYME.	Responsables de garantizar la continuidad operativa y evitar multas por incumplimiento de las leyes 21.719 y 21.663.
Empleados de la PYME	Personal administrativo y operativo que accede diariamente a los sistemas de la empresa.	Son los usuarios finales cuyas credenciales y accesos deben ser protegidos para evitar ataques de suplantación o robo de información.
Personal Técnico / TI	Encargados de la mantención y desarrollo de los sistemas informáticos internos.	Deben integrar la solución de OAuth sin añadir una complejidad excesiva que supere sus capacidades técnicas actuales.
Clientes de la PYME	Titulares de la información personal y transaccional procesada por la empresa.	Stakeholders clave del negocio que dependen de controles de acceso adecuados para garantizar la confidencialidad de sus datos y cumplir con la Ley N° 21.719.

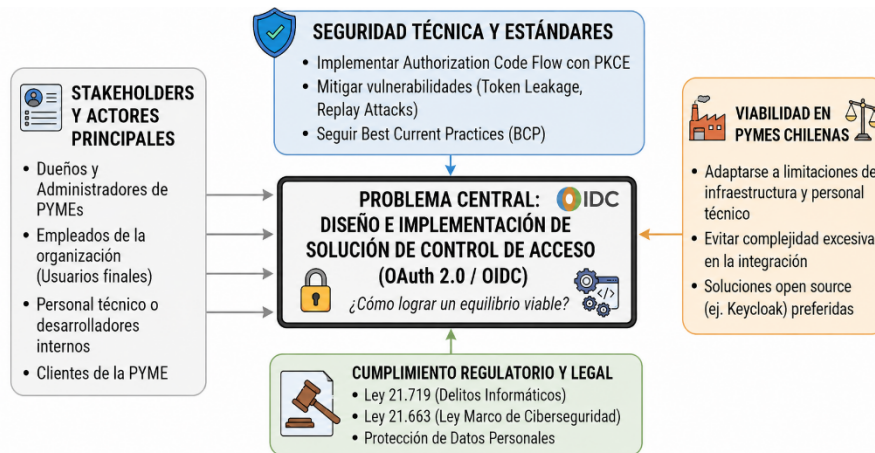


Figura 1: Mapa de Stakeholders.

En la Figura 1 se representa de manera visual la relación entre los distintos *stakeholders*, distinguiendo aquellos que interactúan directamente con la solución tecnológica —como usuarios y personal técnico— de aquellos que forman parte del entorno regulatorio, académico y comercial.

Esta identificación permite comprender que la solución no solo debe ser técnicamente robusta, sino también fácil de implementar, mantener y utilizar, considerando las capacidades reales de las PYMEs. En este sentido, el uso de enfoques basados en la nube, como los servicios de identidad (IDaaS), permite reducir la complejidad técnica y mejorar la viabilidad de adopción por parte de estos actores.

En función de lo anterior, y considerando la necesidad de equilibrar seguridad, usabilidad y cumplimiento normativo, se establecen los objetivos generales y específicos que guiarán el desarrollo de la presente memoria.

1.2 Objetivos

1.2.1 Objetivo general

Proponer y evaluar un diseño de un sistema de control de acceso adecuado para una PYME, basado en mecanismos modernos de autenticación centralizada, autorización y gestión de identidades, que permita mejorar la seguridad en la gestión de usuarios y cumplir con los requerimientos normativos en Chile.

1.2.2 Objetivos específicos

- Analizar el estado actual de los sistemas de autenticación y autorización en entornos web, identificando ventajas y desventajas de su aplicación en pymes.
- Revisar el marco normativo aplicable a pymes en materia de seguridad y protección de datos personales (Ley 21.719 y Ley 21.663).

- Realizar pruebas funcionales para validar la propuesta de solución en distintos escenarios de autenticación, autorización y control de acceso.

1.3 Organización del documento

El presente trabajo de título se encuentra estructurado en los siguientes tres capítulos centrales, los cuales abordan progresivamente el problema de investigación, el marco conceptual, la propuesta de solución y la validación del prototipo desarrollado.

Capítulo 2: Marco Teórico y Conceptual. Describe los conceptos fundamentales relacionados con autenticación, autorización, gestión de identidades, control de acceso basado en roles (RBAC), APIs protegidas y servicios *cloud*. Asimismo, se analizan buenas prácticas de seguridad, vulnerabilidades comunes y el marco normativo chileno aplicable a protección de datos y ciberseguridad.

Capítulo 3: Propuesta de Solución. Presenta el diseño de la solución propuesta y la arquitectura del prototipo desarrollado. Se describen los componentes principales del sistema, la estructura de roles, el modelo de autenticación utilizado y la implementación del prototipo mediante la plataforma Base44, incluyendo la gestión de usuarios y recursos protegidos.

Capítulo 4: Validación de la Solución. Describe las pruebas funcionales realizadas sobre el prototipo para evaluar mecanismos de autenticación, autorización y control de acceso. Además, se presentan los resultados obtenidos, el análisis de seguridad del acceso a la API y consideraciones relacionadas con continuidad operativa, resiliencia y posibles mejoras futuras.

El documento finaliza con conclusiones y un glosario de términos.

CAPÍTULO 2: MARCO CONCEPTUAL

2.1 Sistemas de control de acceso

El control de acceso constituye uno de los pilares fundamentales de la seguridad informática, ya que permite definir qué usuarios, sistemas o servicios pueden acceder a determinados recursos y bajo qué condiciones. Su correcta implementación resulta esencial para proteger información sensible, restringir accesos indebidos y garantizar el cumplimiento de políticas de seguridad dentro de una organización.

En los sistemas modernos de control de acceso, especialmente en entornos digitales distribuidos, resulta fundamental comprender la distinción entre los conceptos de identificación, autenticación y autorización. Estos tres componentes conforman la base de cualquier arquitectura de seguridad orientada a proteger recursos digitales y garantizar un acceso controlado a la información¹.

El correcto diseño e implementación de estos mecanismos es especialmente relevante en el contexto de las PYMEs, donde las limitaciones de recursos técnicos y humanos suelen traducirse en configuraciones de seguridad débiles o incompletas.

2.1.1 Identificación

La identificación corresponde al proceso mediante el cual una entidad declara su identidad dentro de un sistema. Este proceso no implica validación alguna, sino que simplemente permite al sistema reconocer quién está intentando acceder.

Generalmente, esta identificación se realiza a través de elementos como:

- Nombre de usuario
- Correo electrónico
- Identificadores únicos (ID de usuario)

En entornos empresariales, la identificación también puede extenderse a servicios, aplicaciones, dispositivos u otros recursos, no solo a usuarios humanos. Esto cobra relevancia en arquitecturas modernas como microservicios, donde múltiples sistemas interactúan entre sí.

Es importante destacar que una identificación incorrecta o mal gestionada puede derivar en problemas posteriores en la autenticación y en definitiva en el control de acceso, especialmente en sistemas donde no existe una normalización de identidades.

¹ [Qué es el control de acceso y cuál es su importancia](#)

2.1.2 Autenticación

La autenticación es el proceso mediante el cual se verifica que la identidad declarada corresponde efectivamente a la entidad que intenta acceder al sistema².

Este proceso se basa en uno o más factores de autenticación, que tradicionalmente se clasifican en:

- **Algo que el usuario sabe:** contraseñas, PIN
- **Algo que el usuario tiene:** tokens, dispositivos móviles
- **Algo que el usuario es:** biometría

En el contexto de las PYMEs, el método más común sigue siendo el uso de contraseñas. Sin embargo, este enfoque presenta múltiples vulnerabilidades, entre ellas:

- Reutilización de credenciales
- Uso de contraseñas débiles
- Compartición de accesos entre empleados
- Falta de políticas de rotación

Estas debilidades facilitan ataques como *phishing*, *credential stuffing* o accesos no autorizados, lo que evidencia la necesidad de adoptar mecanismos más robustos como autenticación multifactor (MFA) o sistemas federados.

2.1.3 Autorización

Una vez autenticada la identidad de una entidad, la autorización determina qué acciones puede realizar el usuario dentro del sistema³.

Este proceso define el nivel de acceso a recursos, funcionalidades o datos, y se implementa comúnmente mediante algún modelo como RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control) o DAC (Discretionary Access Control)

A diferencia de la autenticación, la autorización no valida quién es el usuario, sino qué está permitido que haga.

En este contexto, OAuth 2.0 se posiciona como un estándar clave, ya que permite implementar autorización delegada, separando completamente la gestión de credenciales del acceso a recursos.

² [Qué es la autenticación](#)

³ [Qué es autorización](#)

2.1.4 Modelos de control de acceso

En entornos modernos, especialmente aquellos basados en aplicaciones web, APIs y servicios distribuidos, los mecanismos de control de acceso adquieren aún mayor relevancia debido al aumento de interacciones entre múltiples usuarios y sistemas. En este contexto, existen distintos modelos de control de acceso ampliamente utilizados, entre los cuales destacan:

- RBAC (Role-Based Access Control).
- ABAC (Attribute-Based Access Control).
- DAC (Discretionary Access Control).

La elección del modelo adecuado depende de factores como la complejidad organizacional, la granularidad requerida, la facilidad de administración y la capacidad técnica disponible para implementar y mantener las políticas de seguridad.

2.1.4.1 Control de Acceso Basado en Roles (RBAC)

El modelo RBAC (Role-Based Access Control) asigna permisos a los usuarios en función de los roles que desempeñan dentro de una organización. En este enfoque, los permisos no se asignan directamente a los usuarios, sino a roles previamente definidos, los cuales agrupan responsabilidades y privilegios.

De esta forma, un usuario obtiene permisos indirectamente al asociarse a uno o más roles organizacionales, permitiendo centralizar la administración de accesos y simplificar la gestión de privilegios.

Una de las principales ventajas de RBAC es su simplicidad de implementación y administración, especialmente en organizaciones donde las funciones de los usuarios están claramente definidas. Además, facilita la auditoría y trazabilidad de accesos, debido a que los permisos se encuentran asociados a estructuras organizacionales comprensibles.

Entre sus beneficios principales destacan:

- Centralización de permisos
- Facilidad de administración
- Escalabilidad
- Mejor trazabilidad y auditoría
- Reducción de errores administrativos

Sin embargo, RBAC también presenta limitaciones. Cuando se requieren reglas muy específicas o contextuales, puede producirse el fenómeno conocido como “explosión de roles”, donde se crean numerosos roles para cubrir distintos escenarios, dificultando la gestión del sistema.

A pesar de estas limitaciones, RBAC continúa siendo uno de los modelos más utilizados en entornos empresariales y sistemas IAM modernos debido a su equilibrio entre seguridad y simplicidad operativa [2][3].

2.1.4.2 Control de Acceso Basado en Atributos (ABAC)

El modelo ABAC (Attribute-Based Access Control) define permisos en función de atributos relacionados con el usuario, el recurso, la acción y el contexto de acceso.

A diferencia de RBAC, donde el acceso depende de roles estáticos, ABAC permite construir políticas dinámicas mediante condiciones lógicas. Por ejemplo, una regla podría establecer que:

“Un usuario puede acceder a un recurso solo si pertenece al área financiera y realiza la solicitud dentro del horario laboral”.

Este enfoque proporciona un nivel mucho más alto de granularidad y flexibilidad, permitiendo adaptar las políticas de seguridad a distintos escenarios organizacionales y contextuales.

Entre sus principales ventajas se encuentran:

- Alto nivel de granularidad
- Políticas dinámicas y adaptativas
- Mejor adecuación a entornos complejos
- Capacidad de incorporar contexto (ubicación, tiempo, dispositivo, etc.)

No obstante, ABAC implica una mayor complejidad técnica tanto en implementación como en mantenimiento. La definición de múltiples atributos y reglas puede aumentar significativamente el esfuerzo administrativo y dificultar las auditorías de seguridad.

Debido a esta complejidad, ABAC suele ser utilizado en organizaciones grandes o entornos donde se requiere un control extremadamente detallado sobre los accesos [4][5].

2.1.4.3 Control de Acceso Discrecional (DAC)

El modelo DAC (Discretionary Access Control) o Control de Acceso Discrecional es un enfoque de seguridad descentralizado en el cual el propietario de un recurso tiene la capacidad de decidir qué usuarios pueden acceder a dicho recurso y qué acciones están autorizados a realizar sobre él.

En este modelo, los permisos son administrados directamente por el dueño del recurso, quien puede otorgar, modificar o revocar accesos según sus necesidades. Esto significa que el control de acceso depende de decisiones individuales realizadas por los usuarios propietarios y no de políticas centralizadas definidas por la organización [6].

DAC es ampliamente utilizado en sistemas operativos tradicionales y sistemas de archivos, donde cada archivo o recurso posee permisos asociados que determinan quién puede:

- Leer información
- Modificar contenido
- Ejecutar archivos

- Compartir recursos con otros usuarios

Una de las implementaciones más comunes de DAC corresponde al uso de Listas de Control de Acceso (ACL), donde cada recurso mantiene una lista que especifica explícitamente qué usuarios o grupos poseen determinados permisos sobre él.

Entre las principales ventajas del modelo DAC se encuentran:

- Simplicidad conceptual
- Facilidad de implementación
- Flexibilidad para compartir recursos
- Administración directa por parte de los usuarios propietarios

Estas características han permitido que DAC sea ampliamente adoptado en entornos pequeños o con estructuras organizacionales simples.

Sin embargo, DAC presenta importantes limitaciones desde el punto de vista de la seguridad organizacional. Debido a que los usuarios tienen capacidad para delegar permisos, existe un mayor riesgo de propagación indebida de accesos, pérdida de control centralizado y configuraciones inconsistentes.

Entre sus principales desventajas destacan:

- Baja escalabilidad en entornos grandes
- Dificultad de auditoría y trazabilidad
- Dependencia de decisiones individuales de usuarios
- Mayor riesgo de otorgamiento excesivo de privilegios
- Escaso control centralizado sobre políticas de acceso

En organizaciones modernas, especialmente aquellas que requieren cumplimiento normativo y control estricto sobre los accesos, DAC suele considerarse insuficiente como modelo principal de seguridad. Esto se debe a que dificulta la aplicación consistente del principio de mínimo privilegio y complica la administración centralizada de permisos.

En el contexto de las PYMEs, DAC puede resultar útil en escenarios simples o de pequeña escala; sin embargo, a medida que aumenta la cantidad de usuarios, aplicaciones y recursos, sus limitaciones administrativas y de seguridad se vuelven más evidentes. Por esta razón, modelos como RBAC son generalmente preferidos en sistemas modernos de gestión de identidades y accesos (IAM), ya que permiten una administración más estructurada, centralizada y escalable.

2.1.4.4 Comparación general de modelos

A continuación, se presenta una comparación general entre los principales modelos de control de acceso analizados:

Tabla 2: Comparación general de modelos de control de acceso

Modelo	Ventajas	Desventajas
RBAC	Fácil de implementar, escalable, simple de auditar	Menor granularidad, posible explosión de roles
ABAC	Alta flexibilidad, control granular, adaptable al contexto	Complejo de implementar y mantener
DAC	Flexible y simple de comprender, permite compartir recursos fácilmente	Baja escalabilidad, difícil administración y menor control centralizado

2.1.4.5 Justificación del modelo seleccionado

Considerando las características de los distintos modelos de control de acceso analizados, se selecciona RBAC (Role-Based Access Control) como enfoque principal para el desarrollo del prototipo propuesto en este trabajo.

La elección se fundamenta en que RBAC ofrece un equilibrio adecuado entre:

- Seguridad
- Facilidad de implementación
- Escalabilidad
- Simplicidad administrativa

Estas características resultan especialmente relevantes en el contexto de PYMEs, donde generalmente existen limitaciones de recursos técnicos, operativos y de personal especializado.

RBAC permite gestionar permisos de forma estructurada mediante roles organizacionales, reduciendo la complejidad administrativa en comparación con DAC (Discretionary Access Control) y evitando la alta complejidad técnica asociada a ABAC (Attribute-Based Access Control). Asimismo, su facilidad de auditoría, trazabilidad y amplia adopción en soluciones modernas de gestión de identidades y accesos (IAM) lo convierten en una alternativa adecuada para sistemas basados en OAuth 2.0 y OpenID Connect.

Adicionalmente, RBAC facilita la aplicación del principio de mínimo privilegio, permitiendo asignar únicamente los permisos necesarios según las funciones de cada usuario dentro de la organización.

No obstante, se reconoce que ABAC podría complementar futuras versiones del sistema en escenarios donde se requiera un mayor nivel de granularidad o control contextual, constituyendo una posible línea de evolución para el prototipo propuesto.

2.2 Evolución de los Mecanismos de Autenticación y Autorización

Para comprender la necesidad de arquitecturas modernas de Gestión de Identidades y Accesos (IAM), es fundamental analizar la evolución histórica de los mecanismos de control de acceso en aplicaciones web y distribuidas. Esta evolución responde a la constante tensión entre la usabilidad, la escalabilidad de la infraestructura y las crecientes exigencias de seguridad de la información.

2.2.1 Autenticación Tradicional Basada en Credenciales

El esquema clásico de autenticación se fundamenta en la combinación de un identificador de usuario y una contraseña (*secret* que solo el usuario conoce). En este modelo, el sistema valida la identidad comparando la credencial ingresada contra un registro almacenado en base de datos local (idealmente utilizando funciones *hash* criptográficas con *salt*, como Bcrypt o Argon2).

A pesar de su simplicidad conceptual e implementación directa, este mecanismo presenta severas vulnerabilidades estructurales en entornos organizacionales y particularmente en PYMES:

- **Factor humano y contraseñas débiles:** Gran parte de los incidentes de seguridad devienen del uso de credenciales de baja entropía o repetidas entre múltiples servicios.
- **Vulnerabilidad a ataques masivos:** Expone a los sistemas a vectores de ataque automatizados como *brute-force*, *dictionary attacks*, *phishing* y *credential stuffing* (uso de listas de credenciales filtradas de otros sitios).
- **Gestión descentralizada de identidades:** Cada aplicación mantiene su propia base de datos de usuarios, lo que incrementa el esfuerzo operacional de administración y revoca accesos de forma tardía o ineficiente ante la desvinculación de personal.

2.2.2 Autenticación Basada en Sesiones e Inconvenientes en Arquitecturas Modernas

Con el auge de las aplicaciones web dinámicas, surgió el modelo de autenticación basado en sesiones (*Stateful Authentication*). Bajo este enfoque, una vez que el servidor valida las credenciales, genera un identificador único de sesión (*Session ID*) que se almacena en la memoria del servidor o en una base de datos de estado (por ejemplo, Redis), devolviendo dicho ID al navegador dentro de una cookie de sesión (usualmente protegida con atributos *HttpOnly* y *Secure*).

Si bien este modelo resuelve el problema de solicitar credenciales en cada petición HTTP, introduce importantes limitaciones en arquitecturas modernas:

- **Falta de escalabilidad horizontal:** Debido a que el estado se mantiene en el servidor, las peticiones subsiguientes del cliente deben ser dirigidas al mismo servidor (*Sticky Sessions*) o se debe sincronizar el almacenamiento de sesiones entre múltiples instancias de la aplicación, añadiendo complejidad y latencia a la infraestructura.

- **Apartamiento de la naturaleza de HTTP:** Vulnera el principio fundamental de diseño del protocolo HTTP como un protocolo sin estado (*stateless*).
- **Limitaciones en clientes heterogéneos:** La dependencia de cookies dificulta la integración nativa con aplicaciones móviles, clientes de terceros o microservicios que consumen directamente APIs RESTful.

2.2.3 Autenticación Desacoplada mediante Tokens de Identidad (JWT)

Para superar los problemas de estado y escalabilidad, la industria adoptó la autenticación basada en tokens (*Stateless Authentication*), cuyo estándar de facto es el formato *JSON Web Token*⁴.

En este esquema, tras verificar las credenciales, el servidor emite un token firmado criptográficamente (mediante clave simétrica HMAC o par de claves asimétricas RSA/ECDSA) que contiene la información del usuario (*claims*), su rol y un tiempo de expiración determinado.

Las principales ventajas e implicancias de este enfoque son:

- **Diseño Stateless:** El servidor no necesita almacenar el token ni mantener una tabla de sesiones activa en memoria. Para validar una solicitud, basta con verificar la firma criptográfica del JWT en cada petición.
- **Estructura autocontenida:** El token viaja típicamente en el encabezado HTTP Authorization: Bearer <token>, permitiendo una integración transparente con APIs REST, clientes móviles y arquitecturas orientadas a microservicios.
- **Desafíos de revocación:** La principal desventaja del modelo con JWT radica en la dificultad de revocar un token antes de su fecha de expiración sin introducir mecanismos adicionales de consulta (listas negras o tablas de invalidación), lo cual reintroduce temporalmente cierto estado al sistema.

2.2.4 De la Autenticación Local a la Autorización Delegada y Federación

A medida que las organizaciones comenzaron a operar múltiples sistemas interconectados y servicios de terceros, los modelos tradicionales de autenticación local demostraron ser insuficientes. Obligar a una aplicación externa a recibir y almacenar las credenciales primarias del usuario para acceder a un recurso representa un riesgo de seguridad inaceptable (*Anti-pattern: Password Sharing*).

Esta necesidad motivó la creación de protocolos estandarizados de **autorización delegada** y **autenticación federada**:

- **OAuth 2.0 (RFC 6749):** Diseñado específicamente para resolver el problema de la *autorización delegada*. Permite a una aplicación cliente obtener acceso limitado a

⁴ [Estándar de JSON Web Tokens](#)

recursos protegidos en nombre del usuario, emitiendo tokens de acceso (*Access Tokens*) sin exponer las credenciales del usuario final al cliente.

- **OpenID Connect (OIDC):** Desarrollado como una capa de *identidad* sobre OAuth 2.0. Agrega la funcionalidad de autenticación mediante un token de identidad estandarizado (*ID Token*) y un punto de acceso centralizado (*UserInfo Endpoint*), haciendo posible el Inicio de Sesión Único (*Single Sign-On* o SSO).

2.2.5 Comparativa de la Evolución Tecnológica de Control de Acceso

A modo de síntesis, la Tabla 3 se presenta una comparación general entre los principales mecanismos analizados:

Tabla 3: Comparación de mecanismos de autenticación y autorización

Mecanismo	Seguridad	Escalabilidad	Complejidad	Adecuación a PYMEs
Credenciales tradicionales	Baja	Baja	Baja	Alta (pero inseguro)
Sesiones	Media	Media	Media	Media
JWT	Media-Alta	Alta	Media	Alta
OAuth 2.0	Alta	Alta	Alta	Alta (con guía adecuada)
OIDC	Alta	Alta	Media-Alta	Alta

2.3 OAuth 2.0 como base para autenticación y autorización moderna

OAuth 2.0⁵ es un *framework* de autorización ampliamente adoptado que permite a aplicaciones acceder a recursos protegidos en nombre de un usuario sin necesidad de compartir directamente sus credenciales [7][8]. Este estándar fue diseñado para abordar las limitaciones de los modelos tradicionales de autenticación, en los cuales las aplicaciones debían manejar contraseñas de los usuarios, incrementando significativamente los riesgos de seguridad.

A diferencia de los enfoques clásicos, OAuth 2.0 introduce un modelo basado en delegación de acceso, donde el usuario autoriza a una aplicación a acceder a ciertos recursos específicos sin revelar sus credenciales. Esta delegación se materializa mediante el uso de *tokens* de acceso, los cuales representan permisos limitados tanto en alcance como en duración.

Este enfoque resulta especialmente relevante en el contexto actual, caracterizado por la proliferación de aplicaciones *web*, APIs y servicios en la nube que requieren interactuar de

⁵ IETF, “The OAuth 2.0 Authorization Framework”, RFC-6749, Octubre 2012.

manera segura. En este escenario, OAuth 2.0 permite desacoplar la autenticación del acceso a recursos, mejorando tanto la seguridad como la escalabilidad de los sistemas.

Uno de los principales beneficios de este modelo es la reducción de la superficie de ataque. Al evitar el almacenamiento y transmisión de contraseñas entre múltiples sistemas, se disminuyen riesgos asociados a filtraciones de credenciales, reutilización de contraseñas y ataques de *phishing*. Asimismo, los *tokens* emitidos poseen una validez temporal limitada y pueden ser revocados, permitiendo un mayor control sobre los accesos.

Además, OAuth 2.0 permite implementar un control de acceso más granular mediante el uso de *scopes* (ámbitos), los cuales definen explícitamente qué recursos o acciones están permitidos para un cliente determinado. Esto facilita la aplicación del principio de mínimo privilegio, asegurando que las aplicaciones solo accedan a la información estrictamente necesaria.

En el contexto de las PYMEs, OAuth 2.0 representa una referencia importante para el diseño de sistemas modernos de autenticación y autorización, permitiendo centralizar el control de acceso, reducir la dependencia de credenciales compartidas y facilitar la integración entre aplicaciones.

Sin embargo, la implementación completa de este estándar puede resultar compleja para organizaciones con recursos técnicos limitados, debido a la necesidad de configurar correctamente flujos de autorización, validación de *tokens* y mecanismos de seguridad adicionales.

Por esta razón, en este trabajo OAuth 2.0 es utilizado principalmente como base conceptual para el diseño de una solución de autenticación centralizada adaptada al contexto de una PYME.

2.3.1 Componentes principales

El modelo de OAuth se compone de los siguientes actores:

- **Resource Owner:** Usuario que posee los datos.
- **Client:** Aplicación que solicita acceso.
- **Authorization Server:** Emite *tokens*.
- **Resource Server:** Protege los recursos.

Adicionalmente, introduce conceptos clave como:

- **Access Tokens:** Pequeño fragmento de código que contiene una gran cantidad de datos. La información sobre el usuario, los permisos, los grupos y los periodos de tiempo está integrada en un único *token* que se transmite desde un servidor al dispositivo del usuario⁶.
- **Refresh Tokens:** Cadena de caracteres que el cliente de OAuth puede usar para obtener un nuevo *token* de acceso sin la interacción del usuario⁷.

⁶ <https://www.okta.com/identity-101/access-token/>

⁷ <https://oauth.net/2/refresh-tokens/>

- **Scopes:** Mecanismo de OAuth 2.0 que permite limitar el acceso de una aplicación a la cuenta de un usuario. Una aplicación puede solicitar uno o más ámbitos; esta información se presenta al usuario en la pantalla de consentimiento, y el *token* de acceso emitido a la aplicación se limitará a los ámbitos concedidos⁸.

Estos elementos permiten controlar de forma granular el acceso a recursos, limitando tanto el alcance como la duración de los permisos otorgados.

2.3.2 Flujos de autorización

OAuth 2.0 define distintos flujos de autorización orientados a distintos tipos de aplicaciones y escenarios de seguridad. Entre ellos, uno de los más utilizados actualmente es el Authorization Code Flow con PKCE (Proof Key for Code Exchange)⁹, considerado una alternativa segura para aplicaciones web y móviles modernas.

Este flujo permite reducir riesgos asociados a la interceptación de códigos de autorización y evita la necesidad de almacenar secretos en aplicaciones públicas.

Entre sus principales ventajas se encuentran:

- Reducción de exposición de *tokens*
- Protección frente a ataques de interceptación
- Compatibilidad con aplicaciones modernas
- Mayor seguridad en autenticación delegada

Debido a sus características de seguridad, este flujo es ampliamente recomendado en arquitecturas modernas basadas en autenticación centralizada.

En el contexto de este trabajo, el flujo Authorization Code con PKCE se considera como referencia conceptual para comprender las buenas prácticas actuales asociadas a autenticación y autorización segura, sin implementar todos los componentes avanzados definidos por el estándar.

2.3.2.1 Acceso del cliente a APIs y mecanismos de seguridad

En arquitecturas modernas basadas en aplicaciones web, es común que el cliente (*frontend*) interactúe directamente con servicios de *backend* mediante el consumo de APIs. Este enfoque permite desacoplar la lógica de presentación de la lógica de negocio, facilitando la escalabilidad y mantenibilidad del sistema.

⁸ <https://oauth.net/2/scope/>

⁹ Definido como parte del estándar OAuth 2.0: IETF, “Proof Key for Code Exchange by OAuth Public Clients” RFC-7636 Septiembre 2015.

Sin embargo, el acceso directo del cliente a *endpoints* de una API introduce riesgos de seguridad que deben ser gestionados adecuadamente. En particular, es fundamental garantizar que únicamente usuarios autenticados y autorizados puedan acceder a los recursos expuestos.

La autenticación en este tipo de arquitecturas suele realizarse mediante mecanismos basados en sesiones o uso de *tokens* que son enviados en cada solicitud HTTP para validar la identidad del usuario.

Adicionalmente, es necesario implementar mecanismos de autorización que permitan controlar el acceso a recursos según los privilegios asignados a cada usuario. Uno de los enfoques más utilizados corresponde al Control de Acceso Basado en Roles (RBAC), el cual permite restringir funcionalidades según el rol definido dentro del sistema u organización.

Por otro lado, cuando el cliente y el servidor operan en otros dominios, resulta necesaria la configuración de políticas de **Cross-Origin Resource Sharing (CORS)**¹⁰, permitiendo controlar qué orígenes pueden acceder a la API y reduciendo riesgos asociados a solicitudes no autorizadas.

Finalmente, el uso de protocolos seguros como HTTPS resulta fundamental para proteger la información transmitida entre cliente y servidor, evitando ataques de interceptación de datos.

En el contexto del prototipo desarrollado, estos mecanismos se aplican de forma simplificada, priorizando la validación conceptual del control de acceso y autenticación centralizada por sobre una implementación empresarial completa

2.4. OpenID Connect (OIDC)

OpenID Connect (OIDC)¹¹ es un protocolo de autenticación que se construye como una capa adicional sobre OAuth 2.0, con el objetivo de proporcionar un mecanismo estandarizado para verificar la identidad de los usuarios [9]. Mientras OAuth 2.0 está orientado principalmente a la autorización —es decir, a determinar qué recursos puede acceder un cliente—; OIDC extiende este modelo para incorporar autenticación, permitiendo así conocer quién es el usuario que interactúa con el sistema.

Esta extensión resulta fundamental en arquitecturas modernas, donde múltiples aplicaciones requieren no solo acceso autorizado a recursos, sino también información confiable sobre la identidad del usuario. En este sentido, OIDC se posiciona como un estándar ampliamente adoptado para la gestión de identidades digitales en entornos web, móviles y de microservicios.

OIDC introduce una serie de componentes adicionales que complementan el modelo de OAuth, siendo el más relevante el **ID Token**. Este *token*, generalmente estructurado en formato JSON Web Token (JWT), contiene información verificable sobre la autenticación del usuario, como su identificador único, el emisor del *token*, el tiempo de expiración y otros

¹⁰ [Uso compartido de recursos entre orígenes \(CORS\)](#)

¹¹ [Que es OpenID Connect](#)

atributos relevantes. A diferencia del Access Token, que se utiliza para acceder a recursos protegidos, el ID Token tiene como propósito principal comunicar información de identidad al cliente.

Además del ID Token, OIDC define otros elementos importantes como:

- **UserInfo Endpoint:** Permite a las aplicaciones cliente obtener información adicional del usuario autenticado, como nombre, correo electrónico u otros atributos, de forma segura.
- **Scopes específicos (openid, profile, email, etc.):** Determinan qué tipo de información será accesible sobre el usuario.
- **Sesiones federadas:** Facilitan la gestión de sesiones entre múltiples aplicaciones, permitiendo mantener el estado de autenticación de forma centralizada.

Entre las principales capacidades que ofrece OIDC se destacan:

- **Autenticación federada:** Permite que los usuarios se autenticuen a través de un proveedor de identidad externo (por ejemplo, Google o Microsoft), reduciendo la necesidad de gestionar credenciales localmente.
- **Uso de tokens de identidad (ID Tokens):** Proporciona un mecanismo seguro y estandarizado para transmitir información de identidad entre sistemas.
- **Centralización de sesiones:** Permite gestionar la autenticación de múltiples aplicaciones desde un único punto, facilitando la implementación de Single Sign-On (SSO).

Estas características permiten reemplazar los sistemas tradicionales de autenticación basados en formularios locales por soluciones centralizadas, lo que no solo mejora la experiencia del usuario, sino que también incrementa significativamente el nivel de seguridad. En lugar de que cada aplicación gestione sus propias credenciales, se delega esta responsabilidad a un proveedor de identidad confiable, reduciendo la superficie de ataque.

En el contexto de las PYMEs, la adopción de OIDC representa una oportunidad para modernizar la gestión de accesos sin necesidad de implementar soluciones complejas desde cero. Al integrarse con OAuth 2.0, permite construir sistemas más seguros, escalables y fáciles de mantener, especialmente cuando se requiere interoperabilidad entre distintas aplicaciones internas o servicios externos.

No obstante, al igual que OAuth, su correcta implementación requiere comprender adecuadamente sus flujos y configuraciones, ya que una mala utilización de los *tokens* o una incorrecta validación de éstos puede introducir vulnerabilidades en el sistema.

En síntesis, OpenID Connect complementa a OAuth 2.0 al incorporar autenticación dentro de un modelo basado en *tokens*, permitiendo construir soluciones modernas de gestión de identidad que equilibran seguridad, usabilidad y escalabilidad.

2.5. Inicio de sesión único (SSO)

El inicio de sesión único o *Single Sign-On* (SSO) es un mecanismo de autenticación que permite a un usuario acceder a múltiples sistemas o aplicaciones mediante una única autenticación inicial [10]. Este enfoque elimina la necesidad de que los usuarios ingresen sus credenciales repetidamente en distintos sistemas, lo que no solo mejora la experiencia de uso, sino que también reduce la complejidad asociada a la gestión de identidades.

Desde una perspectiva técnica, SSO se basa en la confianza entre múltiples aplicaciones (clientes) y un proveedor central de identidad, el cual es responsable de autenticar al usuario y emitir credenciales o *tokens* que serán aceptados por los demás sistemas. Este modelo es particularmente relevante en entornos empresariales donde existen múltiples aplicaciones internas o integraciones con servicios externos.

Sus beneficios en PYMEs incluyen:

- Reducción de credenciales
- Mejora en la experiencia de usuario
- Mayor control de accesos
- Centralización de auditoría

A estos beneficios se suma la disminución de riesgos asociados al uso de contraseñas débiles o reutilizadas, ya que se reduce la cantidad de puntos donde éstas deben ser ingresadas o almacenadas. Asimismo, facilita la revocación de accesos, permitiendo que un cambio en el sistema central se refleje automáticamente en todas las aplicaciones integradas.

El uso de OAuth 2.0 y OpenID Connect permite implementar SSO de manera eficiente, sin necesidad de infraestructuras complejas. En este contexto, OAuth gestiona la autorización de acceso a recursos, mientras que OIDC permite la autenticación del usuario, trabajando en conjunto para ofrecer una solución completa de gestión de sesiones. Esta combinación resulta especialmente adecuada para PYMEs, debido a su flexibilidad, bajo costo de implementación y compatibilidad con arquitecturas modernas.

2.6. Plataformas Cloud de Desarrollo y Servicios de Autenticación Integrada (SaaS/BaaS)

En el desarrollo de software moderno, el modelo de entrega *SaaS* (*Software as a Service*) y *BaaS* (*Backend as a Service*) permite a las organizaciones construir y desplegar aplicaciones utilizando infraestructura y servicios completamente gestionados en la nube. Dentro de este paradigma, las plataformas integran módulos nativos de autenticación (Auth) y gestión de identidades basados en estándares como OpenID Connect (OIDC) y OAuth 2.0. Esto permite delegar la emisión de tokens de seguridad (JWT), el almacenamiento seguro de credenciales y la validación de sesiones a un proveedor cloud, reduciendo la complejidad técnica y eliminando la necesidad de administrar servidores de autenticación locales.

2.7. Gestión de Identidades y Accesos (IAM)

La Gestión de Identidades y Accesos o Identity and Access Management (IAM), en inglés, es un conjunto de políticas, procesos y tecnologías que permiten gestionar identidades digitales y controlar el acceso a recursos dentro de una organización. Su objetivo principal es garantizar que las entidades correctas tengan acceso únicamente a los recursos necesarios, en el momento adecuado y bajo condiciones controladas.

Un sistema IAM moderno incluye:

- Gestión de usuarios
- Autenticación
- Autorización
- Auditoría
- Revocación de accesos

Además de estos componentes, un sistema IAM también contempla aspectos como la gestión del ciclo de vida de las identidades (alta, modificación y baja de usuarios), la federación de identidades y la integración con sistemas internos y externos.

En el contexto de PYMEs, la implementación de IAM suele ser limitada, lo que genera:

- Falta de control de accesos
- Dificultades en auditoría
- Riesgos de seguridad
- Recursos económicos reducidos
- Baja especialización técnica
- Infraestructura limitada

Como consecuencia, muchas organizaciones utilizan mecanismos fragmentados de autenticación y gestión de usuarios, dificultando la administración de accesos y aumentando los riesgos de seguridad.

En este trabajo, los conceptos de IAM son utilizados como referencia para el diseño de un modelo simplificado de gestión de identidades orientado a autenticación centralizada y control de acceso mediante roles.

Debido al alcance del prototipo, no se implementa una solución IAM empresarial completa, sino una aproximación funcional enfocada en demostrar conceptos básicos de autenticación segura y control de acceso adaptados al contexto de una PYME.

2.8. Contexto de aplicación en PYMEs

Las PYMEs presentan características particulares que influyen directamente en la adopción de tecnologías de autenticación y autorización:

- Recursos limitados
- Bajo nivel de especialización técnica
- Infraestructura reducida

Estas condiciones generan barreras para la implementación de soluciones avanzadas como OAuth 2.0, especialmente cuando no existen guías prácticas adaptadas a este tipo de organizaciones.

Entre las problemáticas más comunes se encuentran:

- Uso de autenticación básica
- Falta de centralización
- Baja visibilidad de accesos
- Implementaciones inseguras

Estas prácticas aumentan la exposición a incidentes de seguridad y dificultan la gestión de usuarios dentro de la organización.

Sin embargo, las PYMEs que adoptan correctamente OAuth logran importantes beneficios:

- Mejorar la seguridad
- Reducir riesgos
- Facilitar la gestión de usuarios
- Mejorar la experiencia de uso

Además, la adopción de estos estándares permite una mejor integración con servicios externos, facilita el crecimiento de la organización y contribuye al cumplimiento de normativas de seguridad.

2.9. Arquitectura conceptual de gestión de identidades y control de acceso

La gestión de identidades y control de acceso (i.e., IAM) se basa en una arquitectura que centraliza los procesos de autenticación, autorización y administración de identidades digitales dentro de una organización. Su objetivo es garantizar que únicamente los usuarios o sistemas autorizados puedan acceder a los recursos disponibles, aplicando políticas de seguridad definidas previamente.

En una arquitectura IAM moderna, la autenticación suele ser realizada por un proveedor de identidad (Identity Provider, IdP), mientras que las aplicaciones consumen la información de identidad mediante protocolos estandarizados como OAuth 2.0 y OpenID Connect. Esta separación permite desacoplar la gestión de credenciales de las aplicaciones, reduciendo la complejidad administrativa y mejorando la seguridad del sistema.

De manera general, una arquitectura de gestión de identidades considera los siguientes componentes:

- **Usuario:** entidad que solicita acceso a un recurso.
- **Aplicación cliente:** sistema que requiere autenticar al usuario para proporcionar acceso a sus funcionalidades.
- **Proveedor de identidad (Identity Provider):** servicio responsable de autenticar a los usuarios y emitir las credenciales necesarias para acceder a los recursos.
- **Servidor de recursos o API protegida:** componente que aloja la información o servicios protegidos y valida los permisos de acceso.
- **Mecanismo de autorización:** conjunto de políticas que determinan qué operaciones puede realizar un usuario sobre los recursos disponibles.
- **Tokens de acceso:** credenciales emitidas por el proveedor de identidad que representan la autenticación del usuario y permiten el acceso controlado a los recursos.

En términos generales, el funcionamiento de esta arquitectura comprende las siguientes etapas:

1. El usuario solicita acceso a una aplicación.
2. Si la aplicación reconoce que el usuario no se ha autenticado o tiene un token expirado redirige la autenticación al proveedor de identidad; sino va al paso 5.
3. El proveedor de identidad verifica la identidad del usuario mediante el mecanismo de autenticación configurado.
4. Una vez autenticado, el proveedor de identidad emite uno o más tokens de seguridad.
5. La aplicación utiliza dichos *tokens* para solicitar acceso a los recursos protegidos.
6. El servidor de recursos valida los permisos asociados al *token* antes de autorizar la operación solicitada.

Este enfoque permite implementar autenticación centralizada, reducir la exposición de credenciales, facilitar la integración entre múltiples aplicaciones y aplicar políticas de control de acceso de forma consistente. Además, constituye la base sobre la cual se implementan servicios como *Single Sign-On* (SSO), autenticación multifactor (MFA) y modelos de autorización basados en roles o atributos.

2.10. Marco normativo aplicable a la gestión de identidades y accesos en PYMEs en Chile

El diseño de sistemas de autenticación y autorización no solo debe responder a requerimientos técnicos, sino también a obligaciones legales relacionadas con la protección de datos y la ciberseguridad. En el contexto chileno, las PYMEs deben considerar un marco normativo emergente que establece estándares mínimos para el tratamiento de información y la protección de activos digitales.

Ley 21.719 de Protección de Datos Personales

La Ley 21.719 introduce un nuevo estándar en materia de protección de datos personales, alineándose con regulaciones internacionales como el Reglamento General de Protección de Datos (GDPR)¹².

Entre sus principales implicancias para sistemas de control de acceso se encuentran:

- Necesidad de garantizar la **confidencialidad de los datos personales**
- Implementación de medidas de seguridad proporcionales al riesgo
- Control sobre el acceso a información sensible
- Registro y trazabilidad de accesos

En este contexto, mecanismos como OAuth 2.0 y OpenID Connect contribuyen directamente al cumplimiento de la ley, al permitir:

- Centralizar la autenticación
- Reducir la exposición de credenciales
- Aplicar el principio de mínimo privilegio mediante *scopes*

Ley 21.663 Marco de Ciberseguridad

La Ley 21.663 establece lineamientos generales para la gestión de la ciberseguridad en organizaciones, promoviendo la adopción de buenas prácticas y estándares internacionales¹³.

Desde la perspectiva de gestión de accesos, esta ley enfatiza:

- Protección de sistemas críticos
- Gestión de identidades y accesos como elemento clave de seguridad
- Prevención de accesos no autorizados
- Implementación de controles técnicos y organizacionales

Esto refuerza la necesidad de adoptar soluciones modernas que permitan controlar de forma efectiva quién accede a los sistemas y bajo qué condiciones.

Relación entre el marco normativo y los sistemas IAM

La incorporación de un sistema de gestión de identidades y accesos (IAM) basado en estándares como OAuth 2.0 y OIDC permite a las PYMEs alinear sus prácticas tecnológicas con los requerimientos normativos.

¹² [Ley 21.719: Regula la protección y el tratamiento de los datos personales y crea la agencia de protección de datos](#)

¹³ [Ley 21.663: Ley marco de ciberseguridad](#)

En particular, estos sistemas facilitan:

- Control centralizado de accesos
- Auditoría y trazabilidad de acciones
- Revocación eficiente de permisos
- Implementación de autenticación segura (MFA, SSO)

Síntesis del marco normativo

El marco regulatorio chileno plantea un escenario donde la seguridad de la información deja de ser una práctica opcional para transformarse como normativa en una necesidad organizacional. En este contexto, la adopción de tecnologías modernas de autenticación y autorización no solo mejora la seguridad, sino que también contribuye al cumplimiento normativo.

Por lo tanto, el diseño de la solución propuesta en este trabajo no solo responde a un problema técnico, sino también a una necesidad legal, posicionando la gestión de identidades como un componente estratégico dentro de las PYMEs.

2.11. Síntesis del marco conceptual

El conjunto de conceptos abordados permite comprender cómo los sistemas modernos de control de acceso se estructuran en torno a la gestión de identidades, autenticación segura y autorización delegada.

OAuth 2.0, junto con OpenID Connect, proporciona una base sólida para el desarrollo de soluciones seguras, escalables e interoperables. Estos estándares, en un marco como IAM, permiten separar responsabilidades, mejorar la seguridad y facilitar la integración entre sistemas.

Sin embargo, su correcta implementación en PYMEs requiere considerar sus limitaciones reales, tales como la falta de recursos, conocimiento técnico y herramientas adaptadas a su contexto.

Este trabajo se posiciona precisamente en ese punto, proponiendo una solución que equilibra:

- Seguridad
- Simplicidad
- Adaptabilidad

Con el objetivo de facilitar la adopción de estándares modernos y marcos de seguridad en entornos organizacionales de menor escala, contribuyendo así a mejorar la gestión de accesos y reducir los riesgos asociados a la ciberseguridad.

CAPÍTULO 3: PROPUESTA DE SOLUCIÓN

Para abordar la problemática asociada a la gestión ineficiente e insegura de autenticación y autorización en PYMEs, se propone el diseño e implementación de una solución basada en servicios de identidad en la nube (Identity as a Service, IDaaS), sustentada en los estándares OAuth 2.0 y OpenID Connect (OIDC).

La iniciativa no busca reemplazar plataformas empresariales completas de gestión de identidades, sino demostrar la viabilidad de integrar mecanismos modernos de autenticación y autorización en aplicaciones orientadas a PYMEs mediante el uso de servicios en la nube y estándares abiertos. En este sentido, el trabajo se enfoca en el desarrollo de un prototipo funcional que permita validar conceptos de autenticación centralizada, control de acceso y protección de recursos utilizando OAuth 2.0 y OpenID Connect.

Esta propuesta tiene como propósito principal **centralizar la gestión de identidades y accesos**, eliminando la dependencia de mecanismos tradicionales basados en credenciales locales, los cuales suelen ser vulnerables y difíciles de administrar en entornos con recursos limitados.

En este contexto, la solución busca responder a tres ejes fundamentales:

- **Seguridad:** mediante el uso de estándares modernos y mecanismos robustos de autenticación.
- **Simplicidad:** reduciendo la complejidad técnica para su adopción en PYMEs.
- **Escalabilidad:** permitiendo su crecimiento progresivo sin rediseños estructurales.

Para lograr lo anterior, se define un proceso metodológico estructurado en etapas, el cual permite abordar el problema de forma sistemática, desde la identificación de necesidades hasta la validación de la solución implementada.

Las etapas definidas son:

- Diagnóstico
- Análisis
- Diseño
- Implementación
- Validación
- Despliegue

Este proceso se concibe como iterativo; sin embargo, para efectos de este trabajo se contempla una única iteración, enfocada en el desarrollo de un prototipo funcional que permita validar los conceptos propuestos.



Figura 2: Diagrama del proceso metodológico de desarrollo

3.1 Diagnóstico

La etapa de diagnóstico tiene como objetivo identificar las condiciones actuales de las PYMEs en relación con la gestión de autenticación y acceso a sistemas.

A partir del análisis del contexto, se identifican las siguientes problemáticas recurrentes:

- Uso de múltiples sistemas de autenticación independientes
- Reutilización de contraseñas entre distintas plataformas
- Ausencia de mecanismos de autenticación centralizada
- Falta de control sobre sesiones activas
- Escasa visibilidad sobre quién accede a los sistemas

Estas condiciones no solo afectan la seguridad de la información, sino también la experiencia de usuario, generando fricción en el acceso a servicios digitales.

Asimismo, se identifica que muchas PYMEs no cuentan con capacidades técnicas suficientes para implementar y mantener soluciones IAM complejas de forma local. Esto refuerza la necesidad de utilizar plataformas cloud que permitan integrar autenticación segura mediante configuraciones simplificadas y componentes reutilizables.

3.2 Análisis

En esta etapa se evalúan los riesgos derivados de las problemáticas identificadas en el diagnóstico, así como las limitaciones propias del contexto organizacional.

Entre los principales riesgos se encuentran:

- Compromiso de cuentas por filtración de credenciales
- Accesos no autorizados a información sensible
- Dificultad para revocar accesos de forma centralizada
- Falta de mecanismos de auditoría

Desde una perspectiva técnica, también se identifican barreras relevantes para la adopción de soluciones tradicionales:

- Limitada disponibilidad de recursos técnicos especializados
- Restricciones presupuestarias
- Infraestructura tecnológica reducida

Durante el análisis también se evaluó la posibilidad de implementar un servidor de identidad autogestionado utilizando herramientas *open source*. Sin embargo, esta alternativa implicaba una complejidad técnica considerable relacionada con despliegue, configuración de seguridad, mantenimiento y administración de infraestructura. Debido al alcance del trabajo y a las limitaciones típicas de las PYMEs, se optó por un enfoque basado en servicios *cloud*, priorizando simplicidad de integración, reducción de costos operativos y facilidad de adopción.

En este escenario, se evalúa el uso de plataformas de desarrollo en la nube bajo los modelos *Software as a Service* (SaaS) y *Backend as a Service* (BaaS), las cuales integran nativamente componentes de autenticación (Auth) y compatibilidad con OpenID Connect (OIDC). La selección de una herramienta con estas características (como la plataforma Base44) permite abstraer la infraestructura de identidades y delegar el manejo de credenciales y tokens a un servicio gestionado en la nube. Esto garantiza que el sistema cumpla con estándares de autenticación centralizada y control de accesos sin requerir la configuración ni el mantenimiento de un servidor de identidades dedicado.

3.3 Diseño de la solución

La solución propuesta consiste en el diseño e implementación de un prototipo web para la gestión de acceso a recursos dentro de una PYME, utilizando una arquitectura basada en autenticación centralizada y control de acceso basado en roles (RBAC).

La solución fue desarrollada utilizando la plataforma Base44, la cual permite implementar funcionalidades de autenticación, gestión de usuarios y protección de recursos sin requerir infraestructura propia ni conocimientos avanzados de administración de servidores.

Si bien el prototipo no posee forma completa con todos los componentes de una PYME, implemente de forma implícita OAuth 2.0 y OpenID Connect, su diseño adopta principios alineados con estos estándares, particularmente en lo relacionado con separación entre

autenticación y autorización, gestión centralizada de usuarios y control de acceso mediante roles.

3.3.1 Caso de estudio: Modelo organizacional y roles de la PYME "Dulce Aroma"

Para validar la propuesta conceptual y técnica en un entorno representativo, se tomó como caso de estudio y prueba de concepto a la cafetería "Dulce Aroma", una PYME del rubro gastronómico y comercial. Este entorno demanda la separación de responsabilidades entre la administración del negocio, la operación del personal y el acceso de los clientes finales.

Estructura organizacional y roles del sistema

El prototipo del sistema define tres roles de usuario para el control de acceso basado en roles (RBAC):

- **Propietario / Administrador (admin):** Encargado de la gestión estratégica y operativa del negocio. Responsable legal del tratamiento de datos personales, control total del sistema, aprobación de solicitudes pendientes y administración de usuarios y roles.
- **Empleado (employee):** Personal operativo del local (atendedores y cajeros). Encargado de la atención diaria, procesamiento de pedidos e interacción con el catálogo, sin privilegios administrativos sobre la plataforma ni sobre otros usuarios.
- **Cliente (customer):** Consumidor final o usuario externo que interactúa con la aplicación para consultar la oferta de productos y realizar solicitudes o compras.

Tabla 4: Matriz de funciones y mapeo con el sistema RBAC

Rol en Sistema (Rol)	Módulo / Sección de la App	Permisos y Acciones RBAC
Administrador	• Gestión de Usuarios y Solicitudes pendientes • Catálogo de Productos • Reportes y Configuración Global	Acceso Total (CRUD): Crear, leer, actualizar y eliminar usuarios, modificar roles del sistema, gestionar catálogo y auditoría.
Empleado	• Módulo de Pedidos / Ventas • Consulta de Catálogo e Inventario	Acceso Operativo: Registrar y actualizar estado de pedidos, consultar productos y precios. (Bloqueado para gestión de usuarios o asignación de roles).
Cliente	• Catálogo de Productos • Vista de Pedidos Personales	Acceso Restringido: Consultar productos disponibles, enviar solicitudes de compra y dar seguimiento a sus propios pedidos.

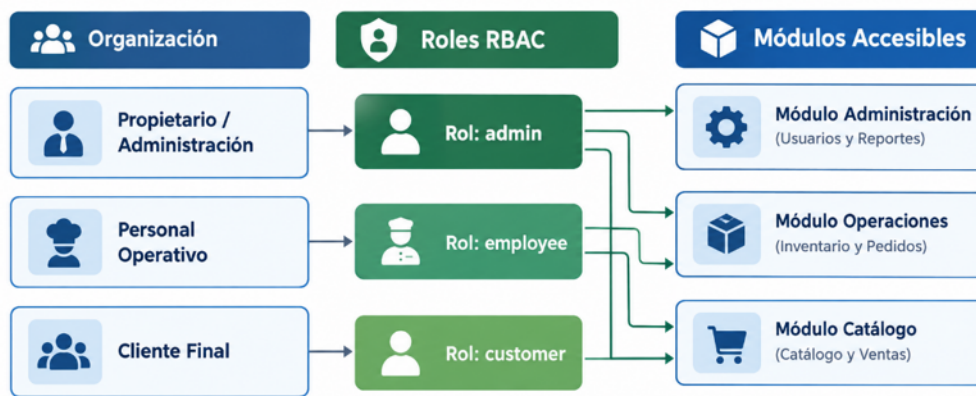


Figura 3: Modelo RBAC Implementado

3.3.2 Principios de diseño

El diseño de la solución se fundamenta en los siguientes principios:

- Centralización de usuarios y accesos.
- Control de acceso basado en roles (RBAC)
- Separación entre autenticación y autorización.
- Protección de recursos mediante validación de sesión.
- Simplicidad de implementación para entornos PYME.
- Escalabilidad para futuras integraciones con estándares como OAuth 2.0 y OpenID Connect.

3.3.3 Arquitectura propuesta

La arquitectura contempla los siguientes componentes:

- Usuario.
- Aplicación Web (Frontend).
- Servicio de autenticación integrado en Base44.
- Base de datos de usuarios.
- Sistema de control de acceso basado en roles (RBAC).
- Recursos protegidos de la aplicación.

En esta arquitectura, la autenticación es gestionada por los servicios proporcionados por Base44, mientras que la autorización se realiza mediante la asignación de roles definidos dentro del sistema.

Cada usuario autenticado accede únicamente a las funcionalidades permitidas según su rol, aplicando el principio de mínimo privilegio.

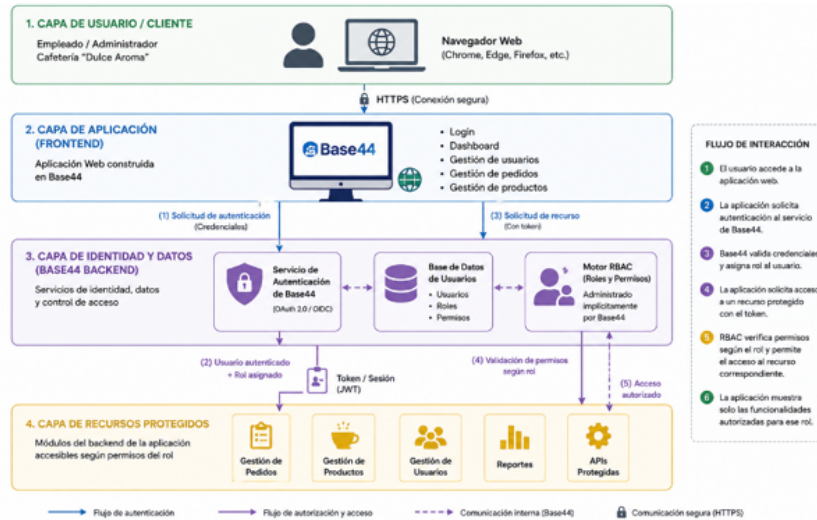


Figura 4: Diagrama de la arquitectura propuesta

3.3.4 Flujo de autenticación

El flujo de autenticación implementado en el prototipo se desarrolla de la siguiente manera:

1. El usuario accede a la aplicación web.
2. Ingresa sus credenciales mediante el formulario de inicio de sesión.
3. El sistema valida las credenciales utilizando los servicios de autenticación de Base44.
4. Una vez autenticado, se crea una sesión activa para el usuario.
5. El sistema identifica el rol asociado al usuario.
6. Se habilitan únicamente las funcionalidades correspondientes a dicho rol.
7. El usuario interactúa con los recursos permitidos según sus permisos.

Este flujo permite controlar el acceso a funcionalidades críticas de la aplicación y centralizar la gestión de usuarios dentro de una única plataforma.



Figura 5: Flujo de autenticación del prototipo

3.4 Tecnologías y herramientas empleadas en la implementación del prototipo

La implementación del prototipo desarrollado en este trabajo requirió la utilización de diversas tecnologías orientadas al desarrollo de aplicaciones web y a la integración de mecanismos modernos de autenticación y control de acceso. La selección de estas herramientas estuvo basada en su facilidad de integración, disponibilidad y capacidad para implementar un entorno funcional que permitiera validar la propuesta.

Las principales tecnologías utilizadas fueron las siguientes:

- **Base44**, como plataforma de desarrollo de aplicaciones web a través de IA.
- **APIs REST**, para la comunicación entre los distintos componentes del sistema [11].
- **OAuth 2.0 y OpenID Connect**, como estándares para la autenticación y autorización.
- **JSON Web Tokens (JWT)**, para la representación segura de la identidad del usuario y la autorización de solicitudes.
- **Control de acceso basado en roles (RBAC)**, para la gestión de permisos según el perfil de cada usuario.
- **RBAC**, implementado para controlar el acceso a las funcionalidades según el rol asignado a cada usuario.

Base44

Esta herramienta fue utilizada como la plataforma principal para el desarrollo del prototipo funcional implementado en esta investigación. Se trata de una plataforma de desarrollo asistida por inteligencia artificial (AI-powered application builder) que permite crear aplicaciones web completas a partir de especificaciones en lenguaje natural, automatizando

gran parte del proceso de desarrollo y reduciendo significativamente el tiempo de implementación [12].

Entre las principales capacidades de Base44 se encuentran la generación de interfaces de usuario, la creación de modelos de datos, la implementación de lógica de negocio, la gestión de bases de datos y la exposición de servicios mediante APIs REST. Asimismo, proporciona herramientas para administrar usuarios, definir permisos de acceso e integrar servicios externos, facilitando el desarrollo de aplicaciones modernas sin requerir la implementación manual de una infraestructura backend compleja.

En el contexto de este trabajo, Base44 permitió construir el prototipo de la aplicación web **"Dulce Aroma"**, utilizada como caso de estudio para validar la propuesta de autenticación centralizada y control de acceso. Gracias a esta plataforma fue posible desarrollar, en un entorno funcional, los módulos de gestión de productos, usuarios, pedidos y reportes, así como implementar un modelo de control de acceso basado en roles (RBAC), diferenciando las funcionalidades disponibles para administradores y empleados.

La utilización de Base44 resultó especialmente adecuada para este trabajo debido a que permitió obtener un prototipo funcional en un tiempo reducido, demostrando que plataformas de desarrollo asistidas por inteligencia artificial pueden constituir una alternativa viable para implementar soluciones de autenticación y control de acceso en pequeñas y medianas empresas, donde habitualmente existen restricciones de tiempo, presupuesto y recursos técnicos.

Además, Base44 abstrae la complejidad del manejo de identidades al integrar nativamente mecanismos de autenticación y el estándar OpenID Connect (OIDC). Esto permite delegar la emisión y validación de tokens de acceso (JWT) directamente a la plataforma, asegurando la identidad del usuario sin la necesidad de desplegar o mantener servidores dedicados de autenticación dentro de la arquitectura.

APIs REST

La comunicación entre los componentes de la solución se realizó mediante servicios REST, utilizando solicitudes HTTP para el intercambio de información entre el cliente y los recursos protegidos. Este enfoque facilita la interoperabilidad y la integración con mecanismos de autenticación basados en estándares abiertos.

OAuth 2.0 y OpenID Connect

La autenticación y autorización fueron implementadas considerando los estándares OAuth 2.0 y OpenID Connect, los cuales permiten delegar el proceso de autenticación a un proveedor de identidad y administrar el acceso a los recursos mediante *tokens*.

JSON Web Tokens (JWT)

Los tokens JWT fueron utilizados para representar la identidad autenticada del usuario y transportar la información necesaria para autorizar el acceso a los recursos protegidos,

permitiendo mantener una arquitectura desacoplada y compatible con aplicaciones distribuidas.

Control de acceso basado en roles (RBAC)

El prototipo implementa un modelo RBAC para restringir el acceso a las funcionalidades de la aplicación según el rol asignado a cada usuario, diferenciando los permisos disponibles para administradores y empleados.

En conjunto, las tecnologías anteriores permitieron desarrollar un prototipo funcional orientado a validar la propuesta de autenticación centralizada y control de acceso planteada en esta investigación.

3.5 Implementación

La implementación del prototipo se realizó utilizando la plataforma Base44, aprovechando sus capacidades de desarrollo *low-code* para construir una aplicación funcional orientada a una PYME.

Las actividades desarrolladas incluyen:

- Diseño de la interfaz de usuario.
- Configuración de autenticación mediante usuarios registrados.
- Implementación de roles para controlar permisos.
- Protección de funcionalidades según privilegios asignados.
- Gestión básica de sesiones de usuario.
- Implementación de módulos representativos de una PYME.
- Validación de acceso a recursos protegidos.

La aplicación desarrollada corresponde a un sistema de gestión para una cafetería denominado “Dulce Aroma”, utilizado como caso práctico para validar el funcionamiento de los mecanismos de autenticación y control de acceso propuestos.

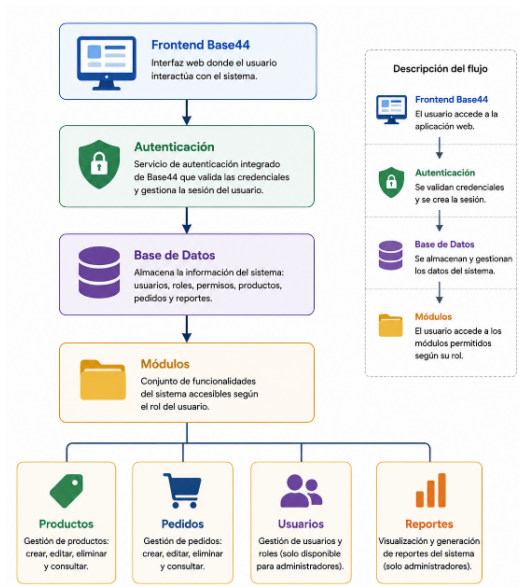


Figura 6: Estructura lógica del prototipo

3.6 Despliegue

El prototipo fue desplegado utilizando la infraestructura proporcionada por Base44, permitiendo su ejecución en un entorno accesible mediante un navegador web.

El despliegue considera:

- Publicación de la aplicación en la nube.
- Gestión centralizada de usuarios.
- Disponibilidad para pruebas funcionales.
- Monitoreo básico de accesos.
- Actualización simplificada del sistema.

Este enfoque elimina la necesidad de administrar servidores propios, reduciendo significativamente la complejidad operativa para una PYME.

3.7 Beneficios de la solución

Entre los principales beneficios obtenidos se encuentran:

- Centralización de la gestión de usuarios.
- Control de acceso basado en roles.
- Reducción de accesos no autorizados.
- Facilidad de administración.
- Menor complejidad técnica para la organización.

- Posibilidad de evolucionar hacia soluciones con mejor infraestructura y otras herramientas en futuras etapas.

Además, se reduce la necesidad de contar con infraestructura propia, lo que disminuye costos y complejidad operativa.

3.8 Evaluación económica y estimación de esfuerzo

Para determinar la factibilidad operativa del prototipo, se estimó un esfuerzo total de desarrollo e implementación de 40 a 53 horas. Este esfuerzo se desglosa en: Configuración inicial y Auth 12–15 Horas, Diseño e implementación de RBAC 15–20 Horas, Pruebas de seguridad e inactividad 8–10 Horas y Despliegue en entorno cloud 5–8 Horas. Desde la perspectiva financiera, el costo de implementación se calcula en un rango de \$600 a \$1.300 USD (\$550.000 a \$1.200.000 CLP aprox.), considerando un valor hora de desarrollo promedio de \$15 a \$25 USD. La operación del sistema contempla un costo de licenciamiento BaaS de \$0 a \$25 USD/mes e implica una mantención estimada de 2 a 4 Horas por mes para administración de roles y permisos (aunque dependiendo del plan pagado por la herramienta estos costes puede variar hasta llegar a \$45 USD/mes)."

3.9 Síntesis de la propuesta

La propuesta desarrollada permite abordar de manera efectiva diversas problemáticas asociadas a la gestión de usuarios y control de accesos en pequeñas y medianas empresas (PYMEs), mediante la implementación de un prototipo web que incorpora mecanismos de autenticación centralizada y autorización basada en roles.

El enfoque adoptado prioriza la construcción de una solución funcional, segura y adaptable a las capacidades técnicas y económicas que caracterizan a este tipo de organizaciones. A diferencia de enfoques tradicionales donde cada sistema administra de forma independiente sus usuarios y credenciales, la propuesta centraliza la gestión de accesos, permitiendo una administración más ordenada, controlada y fácil de mantener.

A través del desarrollo del prototipo se demuestra la viabilidad de implementar mecanismos modernos de gestión de identidades sin requerir infraestructura compleja ni conocimientos avanzados en administración de servidores. Asimismo, la solución permite aplicar principios fundamentales de seguridad como la autenticación de usuarios, la separación entre autenticación y autorización, el control de acceso basado en roles (RBAC) y la protección de recursos según privilegios previamente definidos.

De esta forma, se logra:

- Centralizar la gestión de usuarios y accesos.
- Reducir riesgos asociados al uso inadecuado de credenciales.
- Controlar el acceso a funcionalidades según el rol del usuario.

- Mejorar la administración y trazabilidad de accesos dentro de la organización.
- Facilitar futuras integraciones con mecanismos estandarizados de autenticación y autorización.

Si bien el prototipo no implementa de forma completa una infraestructura basada en OAuth 2.0 y OpenID Connect, su diseño adopta conceptos y principios alineados con estos estándares, constituyendo una base tecnológica que puede evolucionar hacia soluciones más avanzadas de gestión de identidades e integración con proveedores externos de autenticación.

Adicionalmente, la utilización de una plataforma de desarrollo en la nube permite reducir significativamente las barreras técnicas de implementación, eliminando la necesidad de administrar servidores propios, servicios de autenticación dedicados o infraestructura especializada. Esto resulta especialmente relevante para las PYMEs, las cuales suelen enfrentar limitaciones de presupuesto, personal especializado y recursos tecnológicos.

Desde una perspectiva organizacional, la solución propuesta contribuye a fortalecer la seguridad de los sistemas mediante una mejor gestión de usuarios y permisos, permitiendo reducir la exposición a accesos no autorizados y facilitando la administración de cuentas dentro de la empresa. Del mismo modo, favorece la adopción gradual de buenas prácticas de ciberseguridad y gestión de identidades, alineándose con las recomendaciones establecidas en el marco normativo analizado durante esta investigación.

En consecuencia, la propuesta constituye una alternativa viable para mejorar la gestión de accesos en entornos PYME, demostrando que es posible incorporar mecanismos modernos de autenticación y autorización mediante soluciones de baja complejidad operativa. Asimismo, establece una base sólida para futuras extensiones orientadas a integrar estándares como OAuth 2.0 y OpenID Connect, fortaleciendo progresivamente la postura de seguridad de la organización y su capacidad de adaptación a nuevos requerimientos tecnológicos y regulatorios.

CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN Y PRUEBAS DEL PROTOTIPO

4.1 Descripción general del prototipo implementado

Con el propósito de validar la propuesta planteada en el capítulo anterior, se desarrolló un prototipo funcional desplegado sobre una plataforma *cloud* de desarrollo de aplicaciones web. El prototipo simula un sistema de gestión para una pequeña empresa denominada “Dulce Aroma”, permitiendo demostrar la integración de mecanismos modernos de autenticación, autorización y control de acceso en un entorno cercano a un escenario real de uso.

La aplicación incorpora funcionalidades de administración de usuarios, gestión de recursos y control de acceso basado en roles, permitiendo restringir determinadas acciones según el perfil asignado a cada usuario.

La plataforma utilizada proporciona servicios integrados para la autenticación de usuarios, gestión de sesiones, protección de recursos y almacenamiento de información, lo que permite reducir la complejidad técnica asociada a la implementación de infraestructura propia.

El desarrollo del prototipo tuvo como finalidad demostrar la viabilidad de adoptar mecanismos modernos de gestión de identidades dentro del contexto de una PYME, priorizando simplicidad de implementación, seguridad y facilidad de administración.

4.2 Implementación del prototipo

El prototipo fue desarrollado como una aplicación web desplegada en la nube mediante la plataforma Base44. La solución implementa mecanismos de autenticación, gestión de sesiones y control de acceso que permiten proteger funcionalidades específicas de la aplicación según el rol asignado al usuario.

La arquitectura del sistema se compone de los siguientes elementos:

- Aplicación web accesible mediante navegador.
- Servicio de autenticación integrado.
- Base de datos administrada por la plataforma.
- Sistema de gestión de sesiones.
- Control de acceso basado en roles (RBAC).
- Recursos protegidos accesibles únicamente por usuarios autenticados.

Dentro del prototipo se definieron distintos perfiles de usuario para validar restricciones de acceso y comprobar el correcto funcionamiento de las políticas de autorización.

La implementación permitió evaluar de manera práctica la gestión centralizada de identidades y el control de acceso a funcionalidades críticas, replicando necesidades comunes presentes en pequeñas y medianas empresas.

4.3 Pruebas realizadas sobre el prototipo

Con el objetivo de verificar el correcto funcionamiento de la solución implementada, se diseñaron y ejecutaron diversos casos de prueba orientados a validar los mecanismos de autenticación, autorización y control de acceso definidos en la propuesta.

Las pruebas se realizaron sobre el prototipo funcional desarrollado mediante la plataforma Base44, el cual fue desplegado y puesto a disposición en el siguiente enlace:

<https://dulce-aroma-prototipo.base44.app>

Este prototipo corresponde a la aplicación web "**Dulce Aroma**", desarrollada como caso de estudio para esta investigación, e incorpora los mecanismos de autenticación centralizada, control de acceso basado en roles (RBAC) y gestión de usuarios descritos en los capítulos anteriores.

La utilización de un prototipo funcional permitió evaluar el comportamiento de la solución en un entorno cercano a un escenario real de operación, verificando tanto el acceso de los usuarios como la correcta aplicación de las restricciones de autorización definidas para cada rol. Las pruebas descritas en las siguientes secciones fueron ejecutadas directamente sobre esta aplicación, permitiendo validar el cumplimiento de los objetivos planteados para la propuesta.

Las pruebas realizadas fueron las siguientes:

Prueba 1: Registro de usuarios

- Objetivo:
Verificar que nuevos usuarios puedan crear una cuenta dentro del sistema.
- Resultado esperado:
El usuario es registrado correctamente y puede iniciar sesión posteriormente.

Prueba 2: Inicio de sesión válido

- Objetivo:
Comprobar que usuarios registrados puedan autenticarse correctamente.
- Resultado esperado:
El sistema permite el acceso y crea una sesión válida.

Prueba 3: Restricción de acceso a usuarios no autenticados

- Objetivo:
Validar que recursos protegidos no puedan ser accedidos sin autenticación.
- Resultado esperado:
El sistema bloquea el acceso y solicita autenticación.

Prueba 4: Control de acceso basado en roles

- Objetivo:
Verificar que cada usuario acceda únicamente a las funcionalidades permitidas según su rol.
- Resultado esperado:
Las restricciones definidas son aplicadas correctamente.

Prueba 5: Inactividad de sesión (Time-out)

- Objetivo:
Verificar que el sistema aplique automáticamente la terminación de la sesión tras un periodo de inactividad predefinido, mitigando el riesgo de acceso no autorizado en equipos desatendidos.
- Resultado esperado:
El usuario pierde acceso a recursos protegidos hasta autenticarse nuevamente.

4.4 Resultados obtenidos

A continuación, se mostrarán las pruebas hechas en el prototipo y el análisis hechos en cada una de estas en conjunto a sus resultados:

4.4.1 Resultado de la prueba 1: Registro de usuarios

Objetivo

Verificar que un nuevo usuario pueda registrarse correctamente en la plataforma mediante el formulario de creación de cuenta y que sus datos queden almacenados para posteriores procesos de autenticación.

Procedimiento realizado

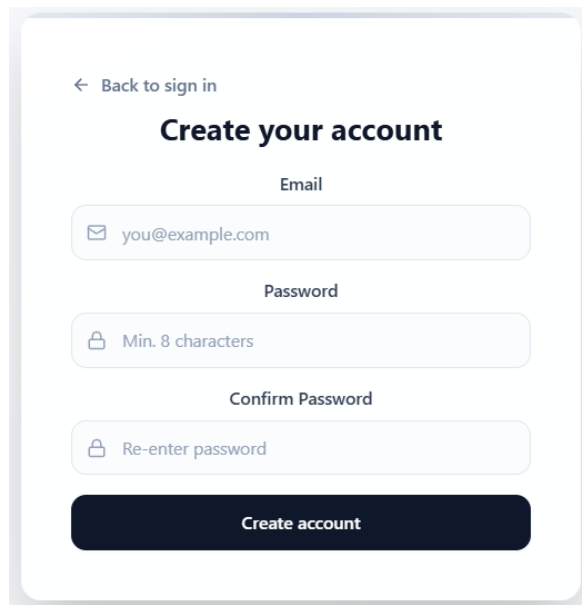
Se accedió a la opción de registro disponible en la plataforma Dulce Aroma.

Posteriormente se ingresaron los datos requeridos por el sistema:

- Nombre
- Correo electrónico
- Contraseña

Una vez completado el formulario, se envió la solicitud de registro y se verificó el comportamiento de la aplicación.

Evidencia



← Back to sign in

Create your account

Email

you@example.com

Password

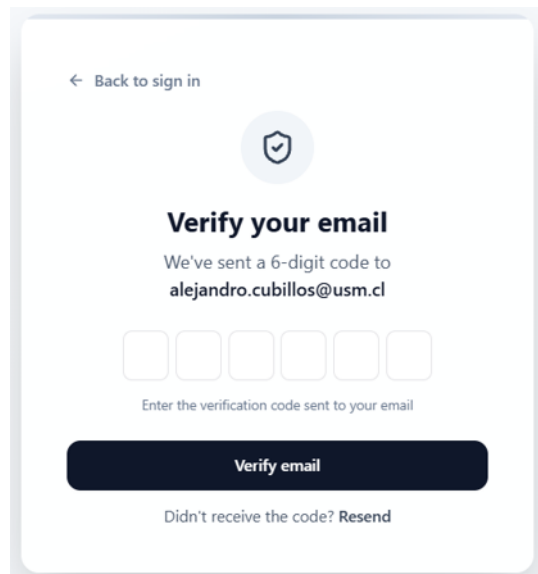
Min. 8 characters

Confirm Password

Re-enter password

Create account

Figura 7: Formulario de registro de usuario



← Back to sign in

✓

Verify your email

We've sent a 6-digit code to
alejandro.cubillos@usm.cl

Enter the verification code sent to your email

Verify email

Didn't receive the code? [Resend](#)

Figura 8: Registro exitoso del usuario

Resultado obtenido

El sistema permitió registrar correctamente al nuevo usuario.

Una vez completado el proceso, la cuenta quedó disponible para utilizar las funcionalidades de autenticación de la plataforma, permitiendo posteriormente iniciar sesión con las credenciales registradas.

No se observaron errores durante el proceso de creación de la cuenta ni problemas asociados al almacenamiento de la información del usuario.

Análisis

Los resultados obtenidos permiten verificar que la plataforma implementa correctamente el proceso de registro de usuarios, proporcionando un mecanismo centralizado para la creación de identidades dentro del sistema.

Este comportamiento constituye un requisito fundamental para la gestión de accesos, ya que permite asociar posteriormente permisos y roles específicos a cada usuario registrado.

Además, el proceso presenta una interfaz simple y comprensible, aspecto especialmente relevante para entornos PYME donde los usuarios pueden no poseer conocimientos técnicos avanzados.

4.4.2 Resultado de la prueba 2: Inicio de sesión válido

Objetivo

Comprobar que los usuarios previamente registrados puedan autenticarse correctamente en la plataforma utilizando sus credenciales de acceso.

Procedimiento realizado

Se utilizó una cuenta registrada previamente en el sistema y se accedió al formulario de inicio de sesión de la plataforma Dulce Aroma.

Posteriormente se ingresaron las credenciales correspondientes:

- Correo electrónico
- Contraseña

Una vez completados los campos requeridos, se seleccionó la opción de inicio de sesión para verificar el comportamiento del sistema.

Evidencia

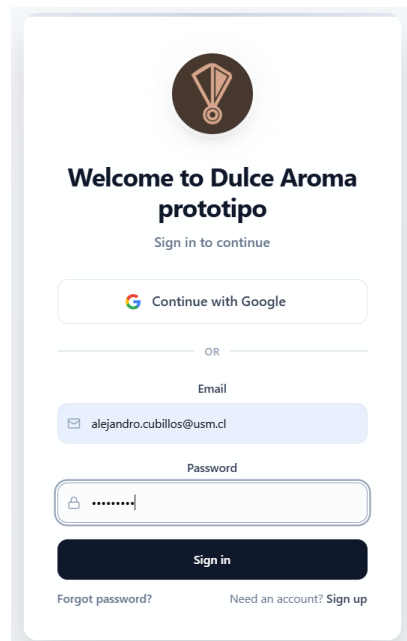


Figura 9: Pantalla de inicio de sesión

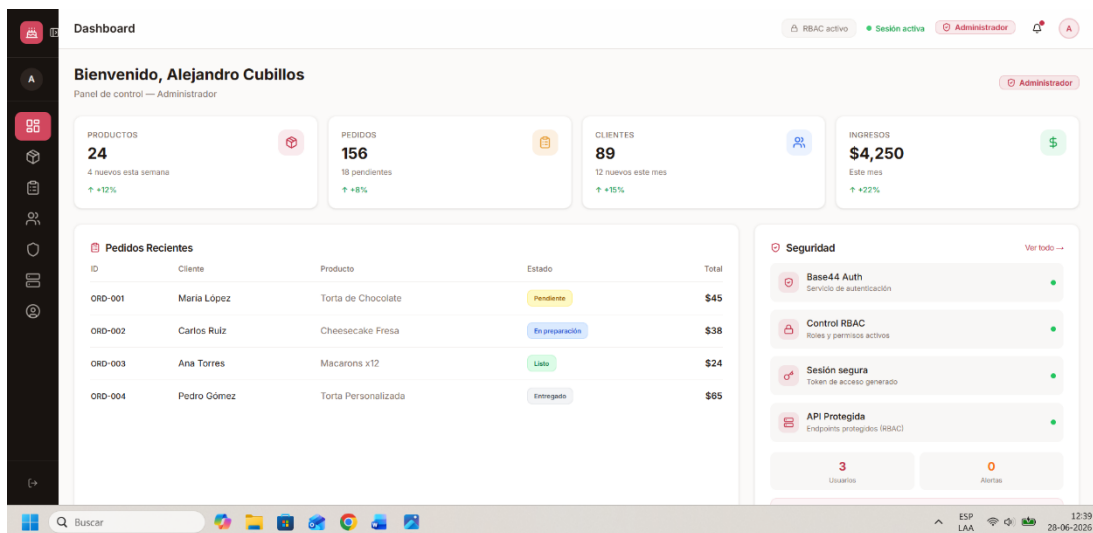


Figura 10: Acceso exitoso al sistema

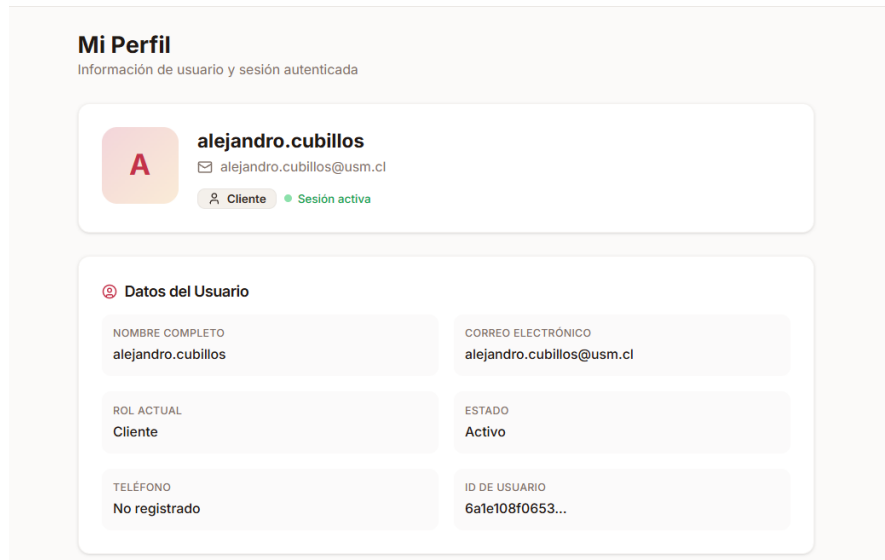


Figura 11: Información del usuario autenticado

Resultado obtenido

El sistema permitió autenticar correctamente al usuario registrado utilizando las credenciales ingresadas.

Tras la validación exitosa de las credenciales, la plataforma redirigió automáticamente al usuario hacia la interfaz principal del sistema, habilitando el acceso a las funcionalidades correspondientes según los permisos asignados.

Durante la prueba no se observaron errores de autenticación, problemas de redirección ni fallas en la creación de la sesión de usuario.

Análisis

Los resultados obtenidos demuestran que el mecanismo de autenticación implementado en la plataforma funciona correctamente para usuarios válidos.

La autenticación constituye uno de los componentes fundamentales de cualquier sistema de gestión de accesos, ya que permite verificar la identidad de los usuarios antes de otorgar acceso a recursos protegidos.

La prueba realizada confirma que el prototipo es capaz de gestionar adecuadamente el proceso de verificación de credenciales y mantener una sesión activa para el usuario autenticado, proporcionando una experiencia de acceso simple y consistente.

Adicionalmente, el funcionamiento correcto de esta característica valida uno de los objetivos principales de la propuesta, relacionado con la centralización y control de acceso a los recursos de la aplicación.

4.4.3 Resultado de la prueba 3: Restricción de acceso a usuarios no autenticados

Objetivo

Validar que los recursos protegidos del sistema no puedan ser accedidos por usuarios que no hayan iniciado sesión previamente.

Procedimiento realizado

Para realizar esta prueba se accedió directamente a una URL protegida del prototipo sin contar con una sesión activa. Previamente se cerró la sesión del usuario para asegurar que no existieran credenciales almacenadas.

Posteriormente se intentó ingresar a funcionalidades que requieren autenticación, tales como:

- Panel principal del sistema.
- Gestión de productos.
- Gestión de pedidos.
- Administración de usuarios.
- Reportes y estadísticas.

Resultado obtenido

El sistema detectó correctamente la ausencia de una sesión válida y bloqueó el acceso a los recursos protegidos.

En lugar de mostrar información sensible o permitir la interacción con funcionalidades internas, la aplicación redirigió automáticamente al usuario hacia la pantalla de autenticación.

No fue posible visualizar datos internos ni ejecutar acciones administrativas sin haber iniciado sesión previamente.

Evidencia

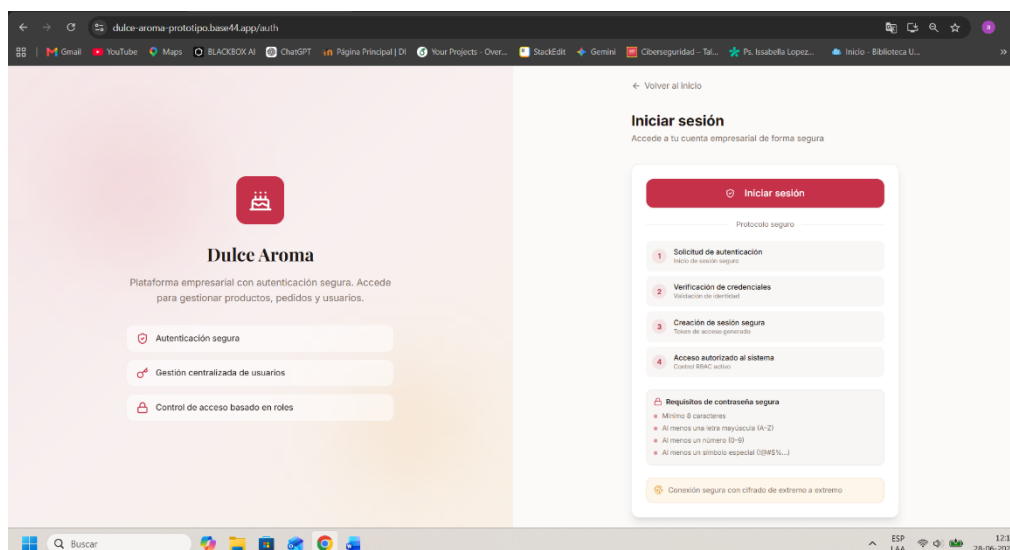


Figura 12: Solicitud de autenticación e inicio de sesión

Análisis

El resultado obtenido evidencia que el prototipo implementa correctamente mecanismos de control de acceso basados en autenticación.

La restricción de acceso evita que usuarios no autorizados puedan consultar información interna o ejecutar operaciones sobre los recursos del sistema, contribuyendo a preservar los principios de:

- Confidencialidad.
- Integridad.
- Control de acceso.

Asimismo, esta funcionalidad permite reducir riesgos asociados a accesos indebidos, exposición de información sensible y utilización no autorizada de funcionalidades administrativas.

Desde la perspectiva de las PYMEs, este mecanismo resulta especialmente relevante, ya que proporciona una capa básica pero efectiva de protección sin requerir configuraciones complejas ni infraestructura adicional.

4.4.4 Resultado de la prueba 4: Control de acceso basado en roles

Objetivo

Verificar que el sistema aplique correctamente las restricciones de acceso según el rol asignado a cada usuario, permitiendo únicamente el acceso a las funcionalidades autorizadas.

Procedimiento

Para realizar esta prueba se crearon cuentas de usuario con distintos roles dentro del sistema. Posteriormente se inició sesión con cada cuenta y se intentó acceder a funcionalidades que corresponden a diferentes niveles de privilegio.

Las acciones evaluadas fueron:

- Acceso al panel principal.
- Acceso a la gestión de productos.
- Acceso a la gestión de pedidos.
- Acceso a la administración de usuarios.
- Visualización de opciones restringidas según rol.

El sistema valida el rol asociado al usuario autenticado antes de permitir el acceso a cada funcionalidad protegida.

Evidencia de la prueba

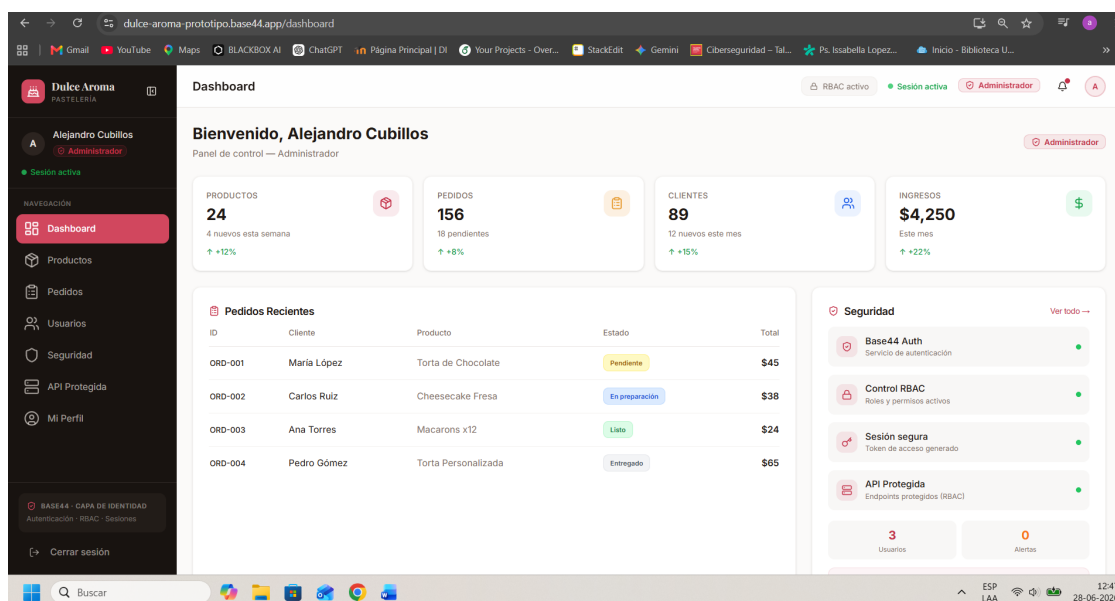


Figura 13: Usuario con permisos de administración

Descripción de la evidencia:

Se observa que el usuario con rol de administrador puede acceder a todas las funcionalidades del sistema, incluyendo gestión de usuarios, productos, pedidos y configuraciones administrativas.

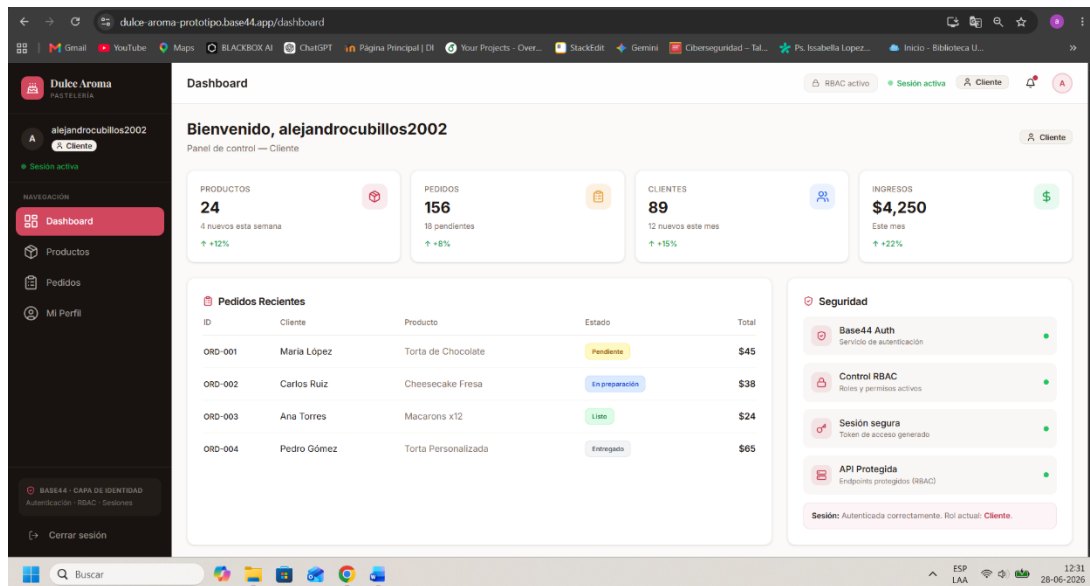


Figura 14: Usuario con permisos restringidos

Descripción de la evidencia:

Se observa que el usuario con rol restringido no visualiza funcionalidades administrativas y únicamente puede acceder a los módulos autorizados para su perfil.

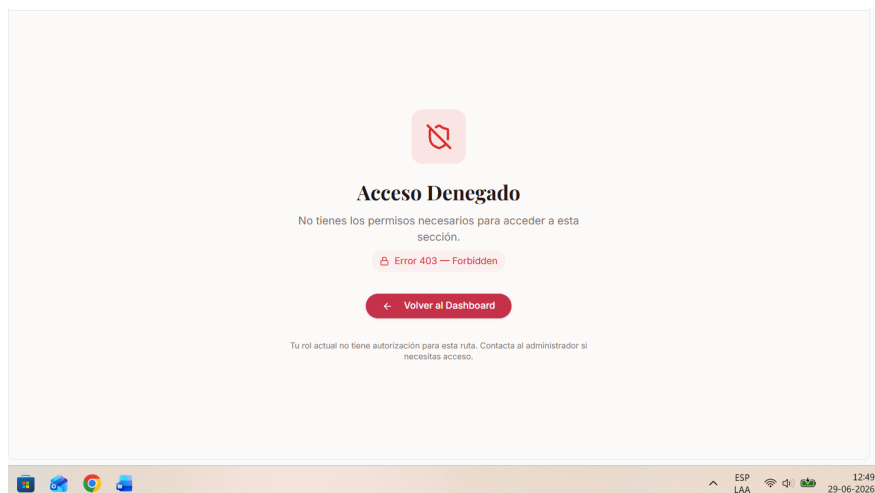


Figura 15: Intento de acceso a funcionalidad no autorizada

Descripción de la evidencia:

Cuando un usuario intenta acceder directamente a una funcionalidad para la cual no posee permisos, el sistema bloquea el acceso y mantiene la protección del recurso.

Resultado obtenido

Durante la prueba realizada se comprobó que el sistema aplica correctamente las restricciones definidas para cada rol.

Los usuarios con privilegios administrativos pudieron acceder a todas las funcionalidades disponibles, mientras que los usuarios con permisos limitados únicamente visualizaron y utilizaron los módulos autorizados.

Asimismo, los intentos de acceso a funcionalidades restringidas fueron rechazados correctamente por el sistema.

Análisis

Los resultados obtenidos demuestran que el modelo RBAC implementado en el prototipo funciona de acuerdo con lo esperado, permitiendo asignar permisos de manera diferenciada según el perfil de cada usuario.

Esta capacidad resulta especialmente relevante para las PYMEs, ya que facilita la aplicación del principio de mínimo privilegio, reduciendo el riesgo de accesos indebidos a información sensible y mejorando la gestión de la seguridad organizacional.

Además, la correcta separación de privilegios contribuye a mejorar la trazabilidad de acciones y constituye una práctica alineada con las recomendaciones de seguridad establecidas por los estándares modernos de gestión de identidades y accesos.

Finalmente, con esta prueba se confirmó que el esquema implementado (RBAC, gestión de tokens y expiración por inactividad) supera de manera sustancial la autenticación tradicional basada únicamente en clave local. Mientras que el modelo tradicional no restringe las acciones internas tras el inicio de sesión, la solución propuesta garantiza el principio de mínimo privilegio, restringiendo el acceso por rol y revocando la sesión automáticamente tras periodos de inactividad.

4.4.5 Resultado de la prueba 5: Inactividad de sesión (Time-out)

Objetivo

Verificar que el sistema aplique automáticamente la terminación de la sesión tras un periodo de inactividad predefinido, mitigando el riesgo de acceso no autorizado en equipos desatendidos.

Procedimiento

Para realizar esta prueba se inició una sesión activa en el sistema. Posteriormente, se mantuvo el navegador en estado de inactividad (sin realizar acciones de teclado, clic o navegación) por un periodo superior al límite configurado. Finalmente, se intentó realizar una acción dentro de la interfaz para comprobar la respuesta del sistema ante la sesión expirada.

Las acciones evaluadas fueron:

- Monitorización del tiempo de inactividad del usuario.
- Activación automática del disparador de cierre de sesión por inactividad.
- Redirección al usuario hacia una vista de "Sesión expirada" o login.

- Invalidación de persistencia de credenciales tras el tiempo límite.

El sistema registra el último evento del usuario y, al exceder el umbral de tiempo permitido, invalida el token de autenticación y fuerza la redirección para proteger la información.

Evidencia de la prueba

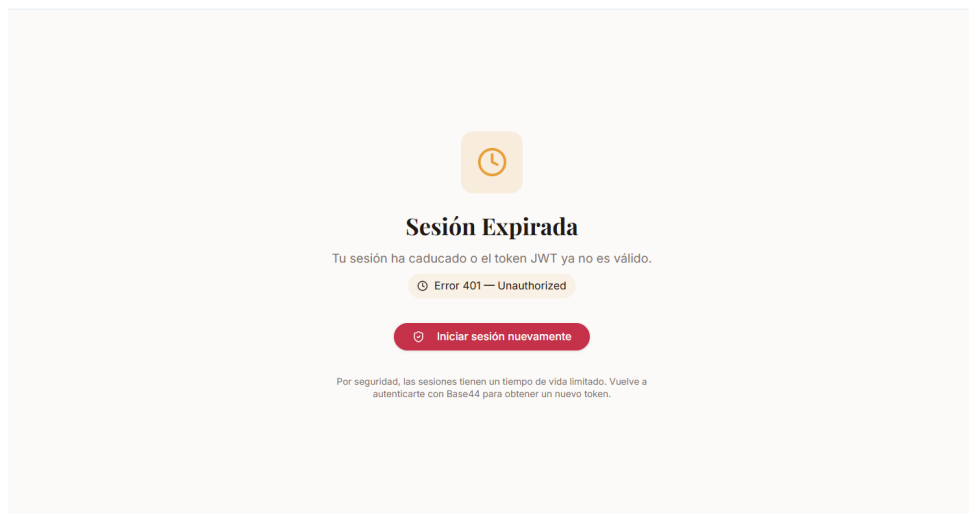


Figura 16: Interfaz de "Sesión Expirada" tras periodo de inactividad

Resultado obtenido

Durante las pruebas realizadas se comprobó que el sistema gestiona correctamente los tiempos de inactividad. Al alcanzar el límite establecido, el sistema invalida automáticamente la sesión, redirigiendo al usuario y evitando cualquier acceso no autorizado sin necesidad de intervención manual por parte del usuario.

Análisis

Esta prueba es fundamental para el trabajo de título, ya que demuestra la implementación de un mecanismo de control de sesión preventivo. A diferencia del cierre manual (que depende del usuario), el control por inactividad protege los datos corporativos ante el olvido del usuario en entornos de alto tráfico o dispositivos compartidos. Esta configuración es un componente clave en la arquitectura de seguridad del prototipo, cumpliendo con las mejores prácticas para el manejo de identidades y la minimización de la superficie de ataque del sistema ante posibles incidentes de seguridad física o lógica.

4.5 Seguridad en el acceso a la aplicación Web

La seguridad del prototipo se basa en mecanismos de autenticación y control de acceso proporcionados por la plataforma utilizada para su desarrollo. Estos mecanismos permiten verificar la identidad de los usuarios antes de otorgar acceso a funcionalidades protegidas del sistema.

El acceso a la aplicación requiere que el usuario disponga de credenciales válidas registradas previamente. Una vez autenticado, la plataforma administra la sesión del usuario y controla el acceso a los recursos disponibles.

Adicionalmente, se implementó un esquema de control de acceso basado en roles (RBAC), permitiendo asignar permisos específicos según el perfil de cada usuario. Este enfoque facilita la aplicación del principio de mínimo privilegio, reduciendo el riesgo de accesos indebidos.

Durante las pruebas realizadas se comprobó que los usuarios no autenticados no pueden acceder a funcionalidades protegidas y que las restricciones definidas para cada rol son aplicadas correctamente.

Estos mecanismos permiten mejorar la seguridad general del sistema y constituyen una base adecuada para futuras integraciones con soluciones IAM más avanzadas basadas en estándares como OAuth 2.0 y OpenID Connect.

4.6 Continuidad operativa y resiliencia

En entornos de pequeñas y medianas empresas (PYMEs), eventos como cortes de suministro eléctrico representan un riesgo relevante para la disponibilidad del sistema. En infraestructuras locales, estos eventos pueden provocar interrupciones del servicio, pérdida de sesiones activas y posibles inconsistencias en los datos.

En contraste, el uso de infraestructura en la nube permite mitigar estos riesgos mediante mecanismos de alta disponibilidad, redundancia y recuperación automática del servicio.

En el contexto del prototipo, el uso de servicios gestionados puede contribuir a mejorar la continuidad operativa mediante el uso de infraestructura y servicios gestionados en la nube, permitiendo aprovechar mecanismos de disponibilidad y administración gestionada proporcionados por la plataforma ante fallas externas. Esto refuerza la decisión de utilizar una plataforma *cloud* para la implementación del prototipo, permitiendo aprovechar mecanismos de disponibilidad, respaldo y administración gestionada sin requerir infraestructura propia.

4.7 Consideraciones sobre autenticación entre servicios

En arquitecturas modernas, es común que distintos servicios interactúen entre sí mediante el consumo de APIs. En estos escenarios, no es recomendable reutilizar *tokens* de usuario para la comunicación entre servicios.

Una alternativa adecuada es el uso del flujo **Client Credentials** de OAuth 2.0, el cual permite a un servicio autenticarse mediante credenciales propias, sin depender de un usuario final.

Si bien esta funcionalidad no fue implementada en el prototipo debido a su complejidad, se identifica como una línea de trabajo futuro relevante para mejorar la seguridad en arquitecturas distribuidas.

CAPÍTULO 5: CONCLUSIONES

El presente trabajo tuvo como propósito proponer y validar una solución de autenticación centralizada y control de acceso para aplicaciones web orientadas a pequeñas y medianas empresas (PYMEs), utilizando estándares abiertos como OAuth 2.0 y OpenID Connect. La investigación permitió analizar los principales desafíos que enfrentan este tipo de organizaciones en la gestión de identidades y accesos, así como desarrollar un prototipo funcional que demostrara la factibilidad de la propuesta.

5.1 Cumplimiento de los objetivos

Los resultados obtenidos durante el desarrollo de esta investigación permiten concluir que la propuesta planteada cumplió satisfactoriamente los objetivos definidos al inicio del trabajo.

Como punto de partida, se realizó un estudio de los mecanismos de autenticación y autorización utilizados en aplicaciones web, analizando su evolución desde enfoques tradicionales basados en credenciales y sesiones hacia soluciones fundamentadas en estándares abiertos. Este análisis permitió identificar las ventajas y limitaciones de cada alternativa, proporcionando la base conceptual para seleccionar una arquitectura de autenticación centralizada orientada al contexto de las pequeñas y medianas empresas.

Posteriormente, se examinó el contexto normativo nacional relacionado con la protección de datos personales y la ciberseguridad, considerando las disposiciones legales vigentes aplicables a las organizaciones chilenas. Este análisis permitió establecer la importancia de incorporar mecanismos que fortalezcan la gestión de identidades y el control de acceso como parte de una estrategia de cumplimiento normativo y protección de la información.

Finalmente, la solución fue materializada mediante el desarrollo de un prototipo funcional construido con la plataforma Base44, sobre el cual se ejecutaron diversos casos de prueba para validar el comportamiento de los procesos de autenticación, autorización y control de acceso. Los resultados obtenidos evidenciaron que los mecanismos implementados respondieron de manera consistente a los escenarios definidos, permitiendo comprobar la viabilidad técnica de la propuesta y su aplicación en un contexto representativo de una PYME.

En conjunto, las actividades desarrolladas durante la investigación permitieron alcanzar el propósito planteado inicialmente, demostrando que la adopción de estándares como OAuth 2.0 y OpenID Connect constituye una alternativa técnicamente factible para fortalecer la gestión de identidades y el control de acceso en aplicaciones web dirigidas a pequeñas y medianas empresas.

Por último, se comprobó operativamente que es viable reemplazar sistemas rudimentarios de contraseña por un control de acceso granular y robusto, demostrando que las aplicaciones para PYMEs pueden alcanzar altos estándares de seguridad sin perjudicar la usabilidad.

5.2 Principales aportes del trabajo

Uno de los principales aportes de esta investigación corresponde al diseño de una arquitectura conceptual de autenticación centralizada y control de acceso especialmente orientada a pequeñas y medianas empresas, considerando sus limitaciones de infraestructura, recursos económicos y capacidades técnicas.

La integración de Auth y OpenID Connect a través de Base44 constituye un aporte clave para el contexto de la PYME, al permitir la adopción de estándares de identidad modernos y seguros sin incurrir en costos elevados de infraestructura ni en sobrecarga de mantención.

Asimismo, el trabajo integra estándares ampliamente utilizados en la industria, como OAuth 2.0 y OpenID Connect, junto con un modelo de control de acceso basado en roles (RBAC), proporcionando una propuesta alineada con las recomendaciones actuales para el desarrollo de aplicaciones web seguras.

Otro aporte importante fue la construcción de un prototipo funcional utilizando la plataforma Base44, el cual permitió materializar la arquitectura propuesta y validar su funcionamiento mediante una aplicación web desarrollada para el caso de estudio "Dulce Aroma". La utilización de esta plataforma permitió reducir considerablemente el tiempo de desarrollo y concentrar los esfuerzos en la implementación y evaluación de los mecanismos de autenticación y autorización definidos en la investigación.

Finalmente, el trabajo demuestra que plataformas modernas de desarrollo asistidas por inteligencia artificial pueden facilitar la adopción de mecanismos avanzados de gestión de identidades y control de acceso, constituyendo una alternativa viable para organizaciones que requieren mejorar su postura de seguridad sin disponer de grandes equipos de desarrollo.

5.3 Limitaciones del trabajo

Si bien la solución propuesta fue validada mediante un prototipo funcional, esta investigación presenta algunas limitaciones que deben ser consideradas.

La evaluación fue realizada sobre un entorno de pruebas y no sobre un ambiente de producción, por lo que no se analizaron aspectos relacionados con rendimiento, escalabilidad, disponibilidad o comportamiento bajo cargas elevadas de usuarios concurrentes.

Asimismo, debido a las características de la plataforma Base44, algunas funcionalidades avanzadas de integración y configuración dependen de capacidades disponibles únicamente en versiones comerciales de la plataforma, lo cual limitó la implementación de ciertos escenarios de autenticación e integración con servicios externos.

Por otra parte, la validación se centró en verificar el correcto funcionamiento de los mecanismos de autenticación y autorización desde una perspectiva funcional, sin realizar pruebas de penetración, auditorías de seguridad o evaluaciones formales frente a ataques reales.

Estas limitaciones no afectan la validez de la propuesta conceptual desarrollada, pero representan oportunidades para continuar ampliando el alcance de futuras investigaciones.

5.4 Trabajo futuro

Como líneas de trabajo futuro, se propone extender la solución incorporando mecanismos avanzados de autenticación multifactor (MFA), autenticación adaptativa y modelos de autorización basados en atributos (ABAC), permitiendo mejorar aún más la seguridad de los accesos.

También resulta de interés implementar la solución en un entorno empresarial real, evaluando su comportamiento con un mayor número de usuarios, aplicaciones y recursos protegidos, además de medir indicadores asociados al rendimiento, disponibilidad y experiencia de usuario.

Adicionalmente, se plantea como trabajo futuro la ejecución de un modelado formal de amenazas basado en la metodología *STRIDE* (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service y Elevation of Privilege). Dado que el presente trabajo se centró en la validación funcional de la arquitectura, resulta relevante aplicar este marco metodológico de manera sistemática sobre la solución propuesta en un entorno de producción o premisas reales. Esto permitirá evaluar y mitigar formalmente riesgos específicos asociados a implementaciones de OAuth 2.0 y OpenID Connect, tales como la suplantación de identidad, la interceptación o fuga de tokens (token leakage), ataques de denegación de servicio (DoS), el uso malintencionado de refresco de tokens (replay attacks) y la elevación de privilegios por configuraciones inadecuadas de scopes. Dicho análisis servirá de base para realizar auditorías de seguridad integrales y pruebas de penetración (pentesting) que fortalezcan la postura de ciberseguridad del sistema.

Finalmente, se propone explorar la integración con otros proveedores de identidad ampliamente utilizados en el ámbito empresarial, como Microsoft Entra ID, Google Identity o Keycloak, evaluando la interoperabilidad de la arquitectura propuesta y su adaptación a distintos contextos organizacionales.

En síntesis, los resultados obtenidos permiten concluir que la propuesta desarrollada constituye una alternativa técnicamente viable para fortalecer la gestión de identidades y el control de acceso en aplicaciones web orientadas a PYMEs, demostrando que la adopción de estándares abiertos como OAuth 2.0 y OpenID Connect facilita la implementación de soluciones más seguras, escalables y alineadas con las buenas prácticas actuales en ciberseguridad.

REFERENCIAS BIBLIOGRÁFICAS

- [1] *PCI Compliance: What to Know About Digital Payment Security*. (2020b, mayo 12). Verizon Enterprise. <https://www.verizon.com/business/resources/articles/small-business-cyber-security-and-data-breaches/>
- [2] Okta. (2024, 12 septiembre). *RBAC vs. ABAC: Definitions & When to Use*. Okta. <https://www.okta.com/identity-101/role-based-access-control-vs-attribute-based-access-control/>
- [3] Lindemulder, G., & Kosinski, M. (2025, 26 noviembre). RBAC. IBM. <https://www.ibm.com/mx-es/think/topics/rbac?>
- [4] McCarthy, M. (2025, 17 octubre). Difference between RBAC vs. ABAC vs. ACL vs. PBAC vs. DAC. *Diferencia entre RBAC vs. ABAC vs. ACL vs. PBAC vs. DAC*. <https://www.strongdm.com/blog/rbac-vs-abac>
- [5] Esteban, A. (2025, 8 mayo). *RBAC vs ABAC: diferencias, cuándo usar cada uno y ejemplos*. Cosmikal. <https://www.cosmikal.es/rbac-vs-abac-ciberseguridad-cual-es-mas-seguro-cuando-usar-cada-uno/>
- [6] NordLayer. (2023, 23 noviembre). *What is discretionary access control (DAC)?* NordLayer. <https://nordlayer.com/learn/access-control/discretionary-access-control/>
- [7] *RFC 6749: The OAuth 2.0 Authorization Framework*. (s.f.). IETF Datatracker. <https://datatracker.ietf.org/doc/html/rfc6749>
- [8] *Tools and Libraries - OAuth 2.0 Simplified*. (2021, 16 diciembre). OAuth 2.0 Simplified. <https://www.oauth.com/oauth2-servers/tools-and-libraries>
- [9] *Final: OpenID Connect Core 1.0 incorporating errata set 2*. (s.f.). https://openid.net/specs/openid-connect-core-1_0.html
- [10] Omondiatieno. (s.f.). *What is single sign-on (SSO) in Microsoft Entra ID? - Microsoft Entra ID*. Microsoft Learn. <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-single-sign-on>
- [11] *REST Security - OWASP Cheat Sheet Series*. (s.f.). https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html
- [12] Base44. (s.f.). Base44. <https://app.base44.com/>
- [13] Jegeib. (s.f.). *Threats - Microsoft Threat Modeling Tool - Azure*. Microsoft Learn. <https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats>

GLOSARIO

ABAC (Attribute-Based Access Control)

Modelo de control de acceso basado en atributos, donde los permisos son definidos mediante reglas dinámicas que consideran características del usuario, recurso, acción o contexto.

ACL (Access Control List)

Lista de control de acceso que define explícitamente qué usuarios o sistemas pueden acceder a un recurso y qué acciones pueden realizar.

API (Application Programming Interface)

Conjunto de reglas y mecanismos que permiten la comunicación e integración entre aplicaciones o sistemas.

Authorization Code Flow

Flujo de autorización definido por OAuth 2.0 que permite obtener tokens de acceso de forma segura mediante un código temporal.

Authentication (Autenticación)

Proceso mediante el cual un sistema verifica la identidad de un usuario o entidad.

Authorization (Autorización)

Proceso que determina qué recursos o acciones están permitidos para un usuario autenticado.

Bearer Token

Tipo de token utilizado en OAuth 2.0 que permite acceder a recursos protegidos mediante el encabezado Authorization.

Backend

Parte de una aplicación encargada de la lógica de negocio, procesamiento de datos y acceso a recursos del sistema.

Cloud Computing

Modelo de provisión de servicios informáticos a través de internet, permitiendo escalabilidad y acceso remoto a recursos.

Credential Stuffing

Ataque informático que utiliza credenciales robadas para intentar acceder a múltiples sistemas mediante reutilización de contraseñas.

CORS (Cross-Origin Resource Sharing)

Mecanismo de seguridad que controla las solicitudes realizadas entre distintos dominios en aplicaciones web.

CSRF (Cross-Site Request Forgery)

Tipo de ataque que induce a un usuario autenticado a ejecutar acciones no deseadas en una aplicación web.

DAC (Discretionary Access Control)

Modelo de control de acceso basado en la asignación de permisos realizada por el propietario de un recurso. Permite otorgar o revocar accesos de manera directa a usuarios o grupos, siendo común en sistemas operativos y sistemas de archivos tradicionales.

Endpoint

Punto específico de acceso a un servicio o API.

Escalabilidad

Capacidad de un sistema para adaptarse al aumento de carga o usuarios sin afectar su funcionamiento.

Frontend

Parte visual e interactiva de una aplicación con la que interactúa el usuario.

HTTPS (HyperText Transfer Protocol Secure)

Versión segura del protocolo HTTP que utiliza cifrado para proteger la información transmitida.

IAM (Identity and Access Management)

Conjunto de políticas y tecnologías destinadas a gestionar identidades y controlar accesos a recursos digitales.

ID Token

Token utilizado en OpenID Connect que contiene información de identidad del usuario autenticado.

JWT (JSON Web Token)

Formato de token compacto utilizado para transmitir información segura entre sistemas mediante firmas digitales.

Logging

Proceso de registrar eventos, acciones o actividades dentro de un sistema informático.

MFA (Multi-Factor Authentication)

Método de autenticación que requiere múltiples factores de verificación para validar la identidad de un usuario.

Microservicios

Arquitectura de software basada en servicios pequeños e independientes que interactúan entre sí.

OAuth 2.0

Framework de autorización que permite a aplicaciones acceder a recursos protegidos sin compartir credenciales directamente.

OIDC (OpenID Connect)

Protocolo de autenticación construido sobre OAuth 2.0 que permite verificar la identidad de un usuario.

OWASP (Open Web Application Security Project)

Organización enfocada en la investigación y difusión de buenas prácticas de seguridad en aplicaciones web.

Phishing

Técnica de fraude utilizada para obtener información sensible mediante engaño.

PKCE (Proof Key for Code Exchange)

Extensión de seguridad de OAuth 2.0 que protege el flujo Authorization Code contra ataques de interceptación.

Proveedor de identidad (Identity Provider)

Sistema encargado de autenticar usuarios y emitir credenciales o tokens de acceso.

PYMES

Pequeñas y medianas empresas.

Rate Limiting

Mecanismo de control que limita la cantidad de solicitudes que un cliente puede realizar a un servicio en un período determinado.

RBAC (Role-Based Access Control)

Modelo de control de acceso basado en roles organizacionales.

Refresh Token

Token utilizado para obtener nuevos tokens de acceso sin requerir nuevamente autenticación del usuario.

Replay Attack

Ataque en el que una solicitud o token válido es reutilizado de forma maliciosa.

Resource Server

Servidor que almacena y protege recursos accesibles mediante OAuth 2.0.

REST API

Tipo de API basada en principios REST para comunicación entre sistemas mediante HTTP.

Role (Rol)

Conjunto de permisos asignados a un usuario dentro de un sistema.

RS256

Algoritmo criptográfico utilizado para firmar digitalmente tokens JWT mediante criptografía asimétrica.

Scope

Permiso o alcance específico otorgado a una aplicación dentro de OAuth 2.0.

Single Sign-On (SSO)

Mecanismo que permite acceder a múltiples aplicaciones mediante una única autenticación.

SPA (Single Page Application)

Aplicación web que carga una única página y actualiza dinámicamente su contenido.

STRIDE

Metodología de análisis de amenazas utilizada para identificar riesgos de seguridad en sistemas informáticos.

Token

Elemento digital utilizado para representar autenticación, autorización o identidad dentro de un sistema.

Validación de Token

Proceso de verificar la autenticidad, integridad y vigencia de un token.

Vulnerabilidad

Debilidad en un sistema que puede ser explotada por un atacante.