UNIVERSIDAD CATÓLICA DE LA SANTÍSIMA CONCEPCIÓN
FACULTAD DE INGENIERÍA
INGENIERÍA CIVIL INFORMÁTICA

PRÁCTICA PROFESIONAL TUTELADA.

Pares&Alvarez, Ingeniería y Proyectos

Pablo Andrés González Keller

Informe de Práctica Tutelada para optar al título de

INGENIERO CIVIL INFORMÁTICA

Supervisor : Oscar Felipe Ulloa Quiroz

Profesor tutor : Braulio Alberto Quiero Hernández

Concepción, 28 de noviembre de 2025.

Dedicatoria

Quiero expresar mi más profundo agradecimiento a mi familia, quienes me acompañaron y apoyaron durante todo este largo proceso lejos de la comodidad de mi hogar, brindándome fortaleza, ánimo y la motivación necesaria para continuar incluso en los momentos más exigentes. Asimismo, agradezco especialmente a mi novia, cuyo cariño, comprensión y apoyo constante fueron un sostén fundamental para avanzar con determinación y mantenerme firme en cada etapa.

Agradecimientos

Agradezco a Pares & Álvarez Ingenieros Asociados S.A. por brindarme la oportunidad de desarrollar mi Práctica Profesional Tutelada en un entorno real de ciberseguridad corporativa. Extiendo un especial agradecimiento a mi supervisor, Oscar Felipe Ulloa Quiroz, por su guía, confianza y permanente disposición para orientarme durante todo el proceso.

A mis amigos, quienes se transformaron en una segunda familia, les agradezco profundamente por acompañarme en mis tardes de soledad, por su compañía sincera y por recordarme que, incluso en los momentos más demandantes, siempre hay espacio para la amistad, el apoyo y las conversaciones que renuevan el ánimo.

Finalmente, agradezco a los docentes y a todas las personas que han contribuido directa o indirectamente a mi formación, por motivarme a alcanzar este objetivo y por fortalecer mis capacidades profesionales a lo largo de estos años.

Resumen

La Práctica Profesional Tutelada se desarrolló en Pares & Álvarez Ingenieros Asociados S.A., empresa de ingeniería con presencia en Chile, Perú y Australia, entre el 28 de julio y el 28 de noviembre de 2025 en modalidad semipresencial. El trabajo se realizó en la Unidad de Ciberseguridad y Tecnologías de la Información.

El propósito central fue **estandarizar la gestión de ciberseguridad** de la organización, alineando procesos y controles con **ISO/IEC 27001:2022**, especialmente en el ámbito de **Gestión de Identidades y Accesos**. Para ello se abordaron tres líneas de acción:

1. **Auditoría de identidades** en Active Directory, Entra ID y Buk.
2. **Actualización normativa** en contraseñas, autenticación y MFA.
3. **Diseño de procedimientos formales** para el ciclo de vida de cuentas corporativas.

Se analizaron más de **1.800 cuentas**, identificándose **600 inconsistencias entre plataformas**, **316 cuentas sin aprovisionamiento adecuado** y **323 cuentas sin uso recurrente**, evidenciando brechas relevantes en control y trazabilidad. A partir de estos hallazgos se desarrollaron entregables críticos: nueva Política de Contraseñas, lineamientos de uso obligatorio de MFA y procedimientos normativos para creación, modificación, baja y auditorías periódicas de cuentas.

La práctica permitió integrar análisis técnico, documentación normativa y aplicación de estándares internacionales, además de fortalecer habilidades profesionales como comunicación, redacción técnica y trabajo colaborativo. En conjunto, los resultados contribuyeron directamente a la **madurez del SGSI**, mejorando la postura de seguridad y estableciendo bases sólidas para la continuidad del proceso de estandarización en Pares & Álvarez.

Abstract

The Tutor-Led Professional Internship was carried out at Pares & Álvarez Ingenieros Asociados S.A., an engineering company with presence in Chile, Peru, and Australia, between July 28 and November 28, 2025, in a semi-in-person modality. The work was conducted within the Cybersecurity and Information Technology Unit.

The central purpose was to standardize the organization's cybersecurity management, aligning processes and controls with ISO/IEC 27001:2022, especially in the field of Identity and Access Management. To achieve this, three lines of action were addressed:

- Identity Audit in Active Directory, Entra ID, and Buk.
- Regulatory Update on passwords, authentication, and MFA.
- Design of formal procedures for the corporate account lifecycle.

More than 1,800 accounts were analyzed, identifying 600 inconsistencies between platforms, 316 accounts without adequate provisioning, and 323 accounts without recurrent use, demonstrating significant gaps in control and traceability. Based on these findings, critical deliverables were developed: a new Password Policy, mandatory MFA usage guidelines, and regulatory procedures for the creation, modification, deletion, and periodic audits of accounts.

The internship allowed for the integration of technical analysis, regulatory documentation, and the application of international standards, in addition to strengthening professional skills such as communication, technical writing, and collaborative work. Overall, the results contributed directly to the maturity of the ISMS (Information Security Management System), improving the security posture and establishing solid foundations for the continuity of the standardization process at Pares & Álvarez.

TABLA DE CONTENIDO

TABLAS

ILUSTRACIONES

Capítulo 1: Introducción

El presente informe corresponde a la Práctica Profesional Tutelada realizada en la empresa Pares & Álvarez Ingenieros Asociados S.A., organización chilena con presencia en Chile, Perú y Australia, dedicada al desarrollo de proyectos de ingeniería y servicios tecnológicos. La práctica fue desarrollada en la Unidad de Ciberseguridad y Tecnologías de la Información, entre el período comprendido del 28 de julio al 28 de noviembre de 2025, en modalidad semipresencial.

Para el desarrollo de la práctica se trabajó con tres plataformas fundamentales para la administración de identidades dentro de la organización. **Active Directory (AD)** corresponde al servicio de directorio utilizado para gestionar cuentas, permisos y autenticación en el entorno local. **Microsoft Entra ID**, plataforma de identidades en la nube, permite administrar accesos, aplicar autenticación robusta y sincronizar usuarios con el entorno local. Por su parte, **Buk** es el sistema de Recursos Humanos utilizado para registrar la dotación institucional, incluyendo altas, bajas y datos contractuales. La comparación y alineación entre estos tres sistemas es clave para garantizar la integridad del ciclo de vida de las cuentas, la trazabilidad de accesos y el cumplimiento de buenas prácticas de seguridad.

Los objetivos fueron los siguientes:

1.1 Objetivo General

El objetivo general de la práctica fue estandarizar la gestión de ciberseguridad de Pares & Álvarez, alineando sus procesos, controles y procedimientos internos con los lineamientos definidos por la norma ISO/IEC 27001:2022, especialmente en el dominio de gestión de identidades y accesos.

1.2 Objetivos específicos

1. Realizar una auditoría completa de identidades en Active Directory (AD), Entra ID y Buk, con el fin de identificar inconsistencias, cuentas inactivas, cuentas sin aprovisionamiento y fallas en los procesos de sincronización.
2. Actualizar la normativa interna de ciberseguridad, elaborando políticas corporativas relacionadas con contraseñas, caducidad de credenciales, uso

obligatorio de autentificadores multi-factor (MFA) y lineamientos de autenticación segura.

3. Diseñar y documentar procedimientos normativos para la gestión de identidades y accesos, formalizando procesos de creación, modificación, baja, control y auditoría de cuentas conforme a buenas prácticas e ISO 27001.

1.3 Metodología de Trabajo

La metodología de trabajo se estructuró bajo el ciclo de mejora continua **PDCA (Plan–Do–Check–Act)**, alineado con las buenas prácticas establecidas por la norma ISO/IEC 27001:2022. En la fase **Plan**, se definieron los objetivos de la práctica, se revisó la normativa vigente y se identificaron las fuentes de información necesarias para la auditoría de identidades. En la etapa **Do**, se ejecutó el análisis de datos provenientes de Active Directory, Entra ID y Buk, además de la elaboración y actualización de políticas y procedimientos. Posteriormente, en la fase **Check**, se realizaron validaciones periódicas mediante reuniones semanales con el equipo de Ciberseguridad y Operaciones TI, revisando hallazgos y ajustando los análisis conforme a las necesidades organizacionales. Finalmente, en la etapa **Act**, se implementaron mejoras a los documentos normativos y se definieron acciones correctivas destinadas a fortalecer los procesos de gestión de identidades.

Este enfoque metodológico permitió desarrollar el trabajo de manera iterativa, garantizando retroalimentación continua y asegurando una alineación efectiva con los estándares internacionales de seguridad de la información.

Capítulo 2: Antecedentes generales de la organización

Pares & Álvarez Ingenieros Asociados S.A. es una empresa chilena fundada en 1992, dedicada a la prestación de servicios de ingeniería multidisciplinaria para sectores como minería, energía, celulosa, infraestructura y procesos industriales. Con más de tres décadas de trayectoria, se ha consolidado como un referente en ingeniería en Chile, participando en proyectos de alta complejidad para compañías como Codelco, BHP y Anglo American. La organización está estructurada bajo una Gerencia General, un Directorio y diversas gerencias técnicas, apoyadas por áreas de soporte como Recursos Humanos, Finanzas, Control de Proyectos, Tecnologías de la Información y Ciberseguridad (Pares & Álvarez Ingenieros Asociados S.A., s.f.).

La organización está estructurada bajo una Gerencia General, un Directorio y diversas gerencias técnicas, apoyadas por áreas de soporte como Recursos Humanos, Finanzas, Control de Proyectos, Tecnologías de la Información y Ciberseguridad.

2.1 Área de Tecnologías de la Información y Ciberseguridad

El área TI está conformada aproximadamente por 30 profesionales, distribuidos en las siguientes unidades: Infraestructura, Operaciones TI, Desarrollo de Software, Soporte técnico, Ciberseguridad.

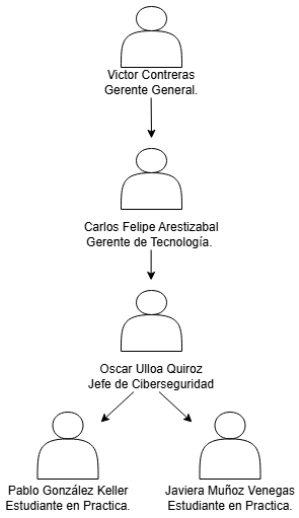

Ilustración 1: Organigrama TI

La Unidad de Ciberseguridad está integrada por:

- El jefe de Ciberseguridad, encargado de la gestión estratégica y operativa.
- Dos estudiantes en práctica profesional, responsables de apoyar tareas de auditoría, análisis, reportes y creación de normativa.

2.2 Tecnologías y herramientas utilizadas durante la práctica

Durante el desarrollo de la práctica se utilizaron diversas plataformas y herramientas tecnológicas esenciales para la gestión de identidades, la administración de accesos y el análisis de información. A continuación, se describen con mayor detalle:

1. **Active Directory (AD):** Active Directory es un **servicio de directorio** desarrollado por Microsoft que permite administrar usuarios, equipos, grupos y permisos dentro de un entorno corporativo. Su función principal es centralizar la autenticación y autorización de usuarios en la red interna. Durante la práctica, AD fue utilizado para **analizar cuentas locales**, identificar cuentas inactivas o duplicadas y contrastar la información con otras plataformas de gestión de identidades para detectar inconsistencias.
2. **Entra ID:** Microsoft Entra ID es un **servicio de gestión de identidades y accesos en la nube**, perteneciente al ecosistema Microsoft Entra. Permite administrar usuarios, aplicar políticas de seguridad modernas, habilitar Autenticación Multifactor (MFA) y sincronizar identidades con Active Directory local. En esta práctica se utilizó Entra ID para **verificar la sincronización de cuentas**, revisar usuarios sin aprovisionamiento, validar configuraciones de MFA y analizar discrepancias respecto de AD y Buk.
3. **Buk (Sistema de Recursos Humanos)**: Buk es una plataforma integral de **gestión de Recursos Humanos**, utilizada para administrar información del personal, como contratos, dotación activa y procesos de ingreso o salida. Dentro del proyecto, Buk fue usado como **fuente oficial de dotación**, permitiendo comparar el estado real del personal con las cuentas existentes en AD y Entra ID, identificando cuentas obsoletas, no aprovisionadas o asociadas a personas desvinculadas.

4. **Excel**: Microsoft Excel fue una de las herramientas principales para el análisis de datos. Se emplearon funciones avanzadas, tablas dinámicas, comparativas masivas, fórmulas condicionales y limpieza de datos para procesar más de 1.800 cuentas provenientes de distintos sistemas. Con Excel se pudieron **detectar patrones, inconsistencias, cuentas inactivas**, y generar reportes ejecutivos con hallazgos relevantes para el área TI y Ciberseguridad.
5. **CrowdStrike Falcon (EDR – Endpoint Detection and Response)**: CrowdStrike Falcon es una plataforma EDR que permite detectar, prevenir y monitorear amenazas en equipos corporativos.
   Aunque no fue utilizada como herramienta principal del análisis de identidades, sirvió como **referencia para validar el estado de dispositivos, endpoints asociados a cuentas y comportamientos anómalos**, complementando la auditoría general del entorno.

Estas herramientas, combinadas, permitieron realizar auditorías de identidad a gran escala, detectar inconsistencias entre sistemas, reforzar la trazabilidad del ciclo de vida de las cuentas y generar documentación técnica alineada a estándares internacionales de seguridad.

Capítulo 3: Descripción detallada de las actividades realizadas

3.1 Auditoría de identidades

se abordó mediante un proceso sistemático que permitió recopilar, depurar y comparar información proveniente de Active Directory, Entra ID y Buk.

El proceso se dividió en cuatro fases principales:

Fase 1: Recolección y consolidación de datos

Se extrajeron listados completos de usuarios desde:

- *Active Directory*, mediante consultas y exportación de atributos (SAMAccountName, descripción, OU, fecha de último inicio de sesión, estado de la cuenta).
- *Entra ID*, utilizando el portal de Azure, exportando usuarios, estado de MFA, licencias, sincronización y propiedades adicionales.
- *Buk*, obteniendo la dotación vigente, usuarios activos, fechas de contratación/desvinculación y datos de RR.HH.

Los tres conjuntos de datos fueron consolidados en Excel, aplicando limpieza de duplicados, estandarización de columnas y normalización de nombres.

Fase 2: Análisis cruzado entre plataformas

Se desarrollaron comparaciones entre cada una de las fuentes utilizando funciones avanzadas de Excel como:

- BUSCARV, XLOOKUP, COUNTIF para detectar usuarios huérfanos
- Power Query para modelar datos y automatizar comparaciones
- Formulas condicionales para categorizar estados de cuentas
- Segmentación por atributos, como sincronización, fecha de actividad, presencia en RR.HH., etc.

Aquí se identificó el origen de las inconsistencias: cuentas antiguas, cuentas sin licencias, usuarios desvinculados que mantenían acceso, cuentas duplicadas por errores de sincronización, entre otros.

Fase 3: Clasificación y priorización de hallazgos

Cada cuenta fue clasificada según:

- Activo / Inactivo
- Sincronizado / No sincronizado
- Usuario vigente / No vigente (según Buk)

- Cuenta huérfana (existe en AD, no existe en Buk)
- Cuenta no aprovisionada (existe en Buk, no aparece en AD/Entra ID)

Esto permitió priorizar qué cuentas representaban mayor riesgo, especialmente las no sincronizadas y sin uso recurrente.

Fase 4: Validación con TI y Ciberseguridad

Los hallazgos fueron revisados semanalmente, clasificando riesgos e identificando fallas en procesos de baja de usuarios. Se elaboraron reportes ejecutivos para cada reunión, incorporando gráficos comparativos, tablas con cuentas críticas y recomendaciones.

Hallazgos principales

- 600 cuentas inconsistentes entre sistemas aproximadamente.
- 316 cuentas sin aprovisionamiento adecuado.
- 323 cuentas sin uso recurrente.

3.2 Actualización de normativa interna de ciberseguridad

El proceso de actualización normativa se realizó siguiendo las directrices de la **ISO/IEC 27001:2022**, específicamente los controles relacionados con autenticación, gestión de identidades y protección de accesos.

Normativas explicadas:

- **Control 5.17 – Uso aceptable de activos:** Define estándares para el uso adecuado de sistemas, incluyendo credenciales, equipos y cuentas.
- **Control 8.10 – Gestión de autenticación:** Exige que la autenticación sea robusta, con contraseñas seguras, MFA y mecanismos de validación consistentes.
- **Autenticación Multifactor (MFA):** es un mecanismo que combina dos o más factores, es decir, por algo que sabes (contraseña), tienes (celular, token) y eres (biometría). Esto fue incorporado como requisito obligatorio en P&A.

- **Llaves de seguridad FIDO2:** son dispositivos físicos que permiten autenticación sin contraseña, reduciendo riesgos de phishing.
- **CIS Benchmarks:** buenas prácticas técnicas que recomiendan configuraciones seguras para Windows, Azure y plataformas de autenticación.

Cómo se realizó el trabajo normativo:

1. **Revisión de documentos existentes** (política de contraseñas antigua, reglamentos internos).
2. **Comparación con requisitos ISO 27001 y CIS**.
3. **Redacción de nuevas políticas** con un formato corporativo estandarizado.
4. **Revisión con TI y Ciberseguridad**, ajustando según operatividad real.
5. **Entrega final** de políticas actualizadas y formateadas.

3.3 Elaboración de procedimientos normativos

Los procedimientos fueron diseñados siguiendo los principios de gestión del ciclo de vida de las identidades:

Etapas del proceso:

1. **Levantamiento de procesos reales** mediante reuniones con TI.
2. **Mapeo de flujo del ciclo de vida de las cuentas** (creación, modificación, baja). y **Documentación formal** en formato corporativo incluyendo a responsables, pasos detallados, controles necesarios y riesgos asociados
3. **Validación del flujo con equipos operativos.**
4. **Corrección y generación de versión final del procedimiento.**

Capítulo 4: Resultados

Durante la práctica se obtuvieron resultados significativos que fortalecieron la gestión de identidades, la estandarización de procesos y la postura de seguridad de la organización. Los avances logrados permitieron cumplir los objetivos planteados inicialmente y generar entregables con impacto directo en el área de Ciberseguridad.

4.1 Resultados de la auditoría de identidades

El análisis de más de 1.800 cuentas provenientes de Active Directory, Entra ID y Buk permitió identificar discrepancias relevantes en el ciclo de vida de las identidades corporativas. Los resultados consolidados se muestran a continuación:

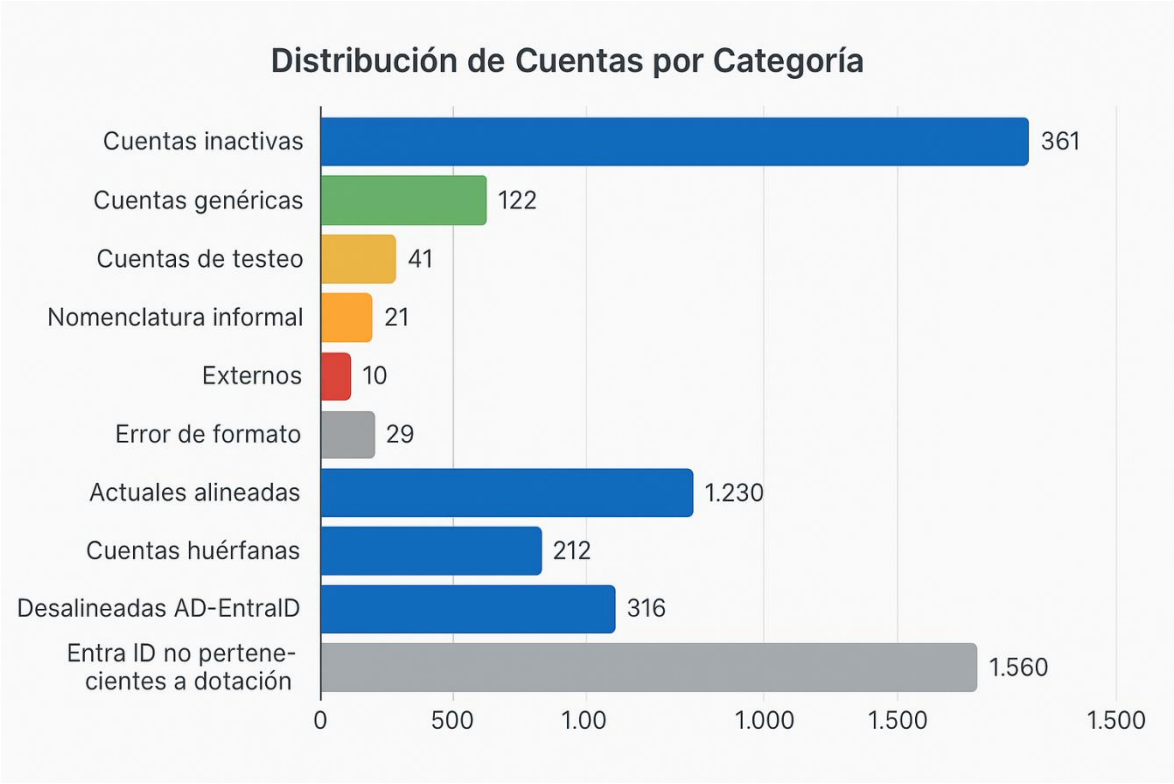

Ilustración 2: Distribución de categorías

Estos hallazgos evidenciaron la necesidad de estandarizar procesos de alta, modificación y baja de usuarios, mejorar la sincronización entre AD y Entra ID, y

robustecer la administración del ciclo de vida de cuentas para reducir riesgos de accesos indebidos.

La auditoría permitió no solo detectar inconsistencias, sino también **modelar su origen**, identificando fallas operativas en procesos de desvinculación, duplicidad de cuentas, cuentas antiguas nunca eliminadas y errores de sincronización entre plataformas locales y la nube.

4.2 Avances normativos

Como resultado del trabajo planificado, se generaron y actualizaron documentos normativos esenciales para el cumplimiento de la norma ISO/IEC 27001:2022. Entre ellos destacan:

- Nueva Política de Contraseñas alineada a los controles 5.17 y 8.10.
- Lineamientos actualizados para el uso obligatorio de Autenticación Multifactor (MFA).
- Recomendación técnica para la adopción de llaves de seguridad FIDO2.
- Procedimientos normativos para creación, modificación, baja y auditoría periódica de cuentas de usuario.

Estos entregables constituyen evidencia concreta del cumplimiento del segundo y tercer objetivo específico, aportando formalidad, trazabilidad y estandarización al Sistema de Gestión de Seguridad de la Información (SGSI).

4.3 Cumplimiento de los objetivos y evolución del plan de trabajo

Los tres objetivos específicos definidos al inicio de la práctica fueron alcanzados satisfactoriamente, aunque su desarrollo implicó ajustes en función de los tiempos, prioridades de la empresa y hallazgos surgidos durante el proceso.

Objetivo	Estado	Descripción del cumplimiento
Auditoría completa de identidades	Cumplido	Se realizó la recolección, limpieza, análisis y comparación de datos entre AD, Entra ID y Buk. El alcance se amplió incorporando análisis adicionales: cuentas duplicadas, usuarios sin MFA y licencias inadecuadas.
Actualización normativa	Cumplido	Se elaboraron documentos normativos completos y se incorporaron correcciones derivadas de reuniones semanales con TI. Se agregaron recomendaciones de CIS Benchmarks que reforzaron el estándar final.
Procedimientos normativos	Cumplido	Se documentaron procesos detallados, se validaron con equipos responsables y se aplicaron mejoras iterativas. Se ampliaron flujos considerando la complejidad real del ciclo de vida de cuentas y se integraron matrices de responsabilidades y puntos de control.

Tabla 1: Objetivos cumplidos.

¿Hubo cambios respecto a la planificación inicial?

Sí, los siguientes:

- Se dedicó más tiempo del previsto a la auditoría, debido al elevado volumen de cuentas y a la detección de inconsistencias no consideradas inicialmente.
- Se añadieron validaciones adicionales por parte del área TI para asegurar que los documentos normativos reflejaran correctamente la operación real.
- Se incorporaron mejoras sugeridas por Operaciones TI, lo que incrementó la calidad final de los procedimientos.

Estos ajustes fueron necesarios para asegurar un resultado más completo y ajustado a las necesidades reales de la organización.

4.4 Aprendizajes técnicos y profesionales.

Durante la práctica se adquirieron diversos aprendizajes relevantes tanto a nivel técnico como profesional, los cuales contribuyeron directamente al desarrollo del trabajo y al cumplimiento de los objetivos.

Aprendizajes técnicos

Análisis avanzado en Excel	manejo de grandes volúmenes de datos, uso de Power Query, funciones de comparación, segmentación y automatización de flujos.
Gestión de identidades	comprensión del ciclo de vida de cuentas, sincronización AD–Entra ID, detección de inconsistencias, uso de MFA y análisis de riesgos asociados.
Normativa ISO/IEC 27001	comprensión del dominio de Identidades y Accesos, controles aplicables, documentación formal y alineación con buenas prácticas.
Ciberseguridad aplicada	identificación de vectores de riesgo, criterios de criticidad y relación entre políticas, procedimientos y controles técnicos.

Tabla 2: Aprendizajes técnicos.

Aprendizajes profesionales

Redacción técnica formal.	elaboración de políticas, procedimientos, reportes ejecutivos y documentación con lenguaje profesional.
Trabajo colaborativo.	interactuando con equipos multidisciplinarios como TI, Ciberseguridad y Operaciones.
Gestión del tiempo.	debido a la necesidad de cumplir con entregas semanales, seguimiento de avances y ajustes en las prioridades
Adaptación y resolución de problemas.	frente a datos incompletos, inconsistencias o procesos no documentados previamente.

Tabla 3: Aprendizaje profesional.

Capítulo 5: Reflexión

Esta práctica profesional fue la oportunidad perfecta para conectar la teoría con la realidad. Participar activamente en auditorías, analizar identidades y coordinar con equipos multidisciplinarios me permitió comprender cómo los conocimientos de la universidad se transforman en soluciones tangibles dentro de una industria tan exigente como la ciberseguridad.

Al trabajar directamente con sistemas como Active Directory, Entra ID y Buk, valoré enormemente lo aprendido en **Redes de Computadores**. Entender la estructura interna, los dominios y las arquitecturas híbridas fue clave para interpretar los hallazgos de las auditorías y proponer mejoras con fundamento. Del mismo modo, las asignaturas de **Ingeniería de Software** me dieron la base para crear políticas y documentación con un enfoque formal y estructurado.

Quiero destacar la utilidad del **Taller de Ingeniería de Software** en el desarrollo de mis habilidades blandas. Gracias a eso, pude desenvolverme con seguridad en reuniones, levantar requerimientos y traducir información técnica para que fuera comprensible en distintos niveles de la empresa.

Más allá de lo técnico, esta experiencia puso a prueba mi ética y capacidad de adaptación. Manejar información sensible y confidencial exigió una responsabilidad constante, mientras que resolver inconsistencias en los datos me obligó a desarrollar un pensamiento crítico y analítico. También aprendí a priorizar y adaptarme a los ritmos ágiles del área TI sin perder la calidad en las entregas.

En cuanto al trabajo en equipo, la interacción con las áreas de Ciberseguridad y Operaciones TI fue enriquecedora. Entendí que la negociación, la escucha activa y saber justificar una decisión técnica son tan importantes como el código mismo.

Pude aplicar el ciclo completo de la ingeniería: concebí enfoques de análisis, diseñé políticas alineadas a estándares, implementé controles de validación y ayudé a operar un sistema de gestión continuo. No fue solo un ejercicio académico; fue una inmersión real en el funcionamiento de un SGSI.

Finalmente, me siento orgulloso de haber generado un aporte real para Pares & Álvarez. El levantamiento de inconsistencias, la nueva documentación y la estandarización de procesos son activos que quedan en la empresa y que facilitarán

la toma de decisiones estratégicas. Esta práctica no solo consolidó mi formación, sino que me dio la confianza para enfrentar futuros desafíos profesionales con una visión técnica, ética y estratégica.

Capítulo 6: Conclusiones

Mi Práctica Profesional Tutelada en **Pares & Álvarez** me permitió cumplir satisfactoriamente con los objetivos propuestos, logrando resultados concretos tanto en el fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) como en la gestión de identidades corporativas. Mi trabajo combinó auditoría técnica, análisis masivo de datos y revisión normativa, contribuyendo directamente a elevar la madurez de la organización bajo los lineamientos de la norma ISO/IEC 27001:2022.

Uno de mis aportes más significativos fue la auditoría integral de identidades en Active Directory, Entra ID y Buk, donde analicé más de **1.800 cuentas corporativas**. Este levantamiento me permitió detectar cerca de **600 inconsistencias** entre plataformas, **316 cuentas** sin la debida sincronización en la nube y **323 cuentas** inactivas por más de seis meses. Estos hallazgos evidenciaron brechas críticas en el ciclo de vida de los usuarios y proporcionaron a la organización una visión cuantificada y real de su estado actual, reduciendo riesgos de accesos indebidos y facilitando la toma de decisiones estratégicas.

Asimismo, cumplí con la actualización del marco normativo interno. Elaboré y revisé documentos esenciales como la Política de Contraseñas, los lineamientos de MFA y el uso de llaves FIDO2. Con esto, logré alinear los controles de la empresa con los requisitos **5.17 y 8.10 de la ISO/IEC 27001**, robusteciendo la protección contra ataques de ingeniería social y accesos no autorizados.

En cuanto a la estandarización de procesos, desarrollé procedimientos formales para la creación, modificación y desactivación de usuarios. Al establecer flujos claros y roles definidos, entregué una guía replicable que no solo reduce errores operativos en el equipo TI, sino que deja una base sólida para futuras auditorías y para la mejora continua del SGSI.

A nivel personal, esta experiencia fue fundamental para consolidar mis habilidades técnicas en análisis de datos, gestión de entornos híbridos e interpretación normativa. Además, la interacción diaria con las áreas de TI y Ciberseguridad fortaleció mi capacidad de comunicación, trabajo en equipo y adaptación.

En resumen, los objetivos fueron alcanzados plenamente. Para **Pares & Álvarez**, mi trabajo deja un entorno de identidades más ordenado, seguro y documentado. Para mí, esta práctica representó el puente definitivo entre la academia y el mundo profesional, brindándome la experiencia y confianza necesarias para desarrollarme como ingeniero en el ámbito de la ciberseguridad.

Referencias

Normativas y estándares

- **ISO/IEC.** (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.
- **ISO/IEC.** (2022). ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. International Organization for Standardization.
- **Microsoft. (2024). Microsoft Entra ID: Identity management and access control documentation.** https://learn.microsoft.com/en-us/entra/id/
- **Center for Internet Security (CIS).** (2023). CIS Benchmarks: Microsoft Windows & Azure. https://www.cisecurity.org/

Marco contextual

- **CSIRT de Gobierno de Chile.** (2024). *Informe anual de incidentes de ciberseguridad en Chile.* Gobierno de Chile. https://csirt.gob.cl/
- **CrowdStrike.** (2024). *Falcon Platform Documentation.* https://www.crowdstrike.com/
- **Pares & Álvarez.** (2025). *Sitio corporativo – Información general de la empresa.* https://www.pya.cl/

Anexos

Glosario

Active Directory (AD): Servicio de directorio utilizado para administrar usuarios, grupos, equipos y políticas dentro de entornos corporativos basados en Windows.

Activos Críticos: Información, sistemas o recursos esenciales para la continuidad operativa y la seguridad de la organización.

Aprovisionamiento: Proceso de creación y habilitación inicial de una cuenta corporativa y sus permisos asociados.

Auditoría de Identidades: Proceso de revisión y validación del estado, coherencia y uso de cuentas en sistemas corporativos.

Buk: Plataforma de gestión de recursos humanos que centraliza información de personal y procesos administrativos.

Ciberseguridad: Disciplina encargada de proteger sistemas, redes y datos frente a amenazas digitales.

Ciclo de Vida de Identidades: Etapas que atraviesa una cuenta corporativa desde su creación hasta su desactivación.

Control 5.17: Control de ISO/IEC 27001 relacionado con la autenticación segura de usuarios.

Control 8.10: Control de ISO/IEC 27001 enfocado en la correcta gestión de credenciales.

Continuidad Operativa: Capacidad de una organización para mantener funciones críticas ante incidentes o interrupciones.

Cuenta Inconsistente: Identidad cuyo estado difiere entre AD, Entra ID y Buk.

Cuentas Huérfanas: Cuentas activas sin un usuario válido asociado o sin respaldo administrativo.

Datos No Recurrentes: Cuentas o accesos sin actividad durante un periodo prolongado.

Datos Sensibles: Información que por su naturaleza requiere estricta protección y control.

Desaprovisionamiento: Proceso de deshabilitar o eliminar una cuenta cuando ya no es requerida.

Documentación Formal: Documentos técnicos elaborados bajo estándares de claridad, estructura y control de versiones.

Entra ID (Azure AD): Servicio de gestión de identidades en la nube de Microsoft.

FIDO2: Estándar de autenticación sin contraseña basado en llaves físicas de seguridad.

Flujo de Trabajo (Workflow): Secuencia estructurada de actividades que conforman un proceso.

Gestión de Identidades: Conjunto de procesos relacionados con la administración de cuentas corporativas.

Hallazgos: Resultados o evidencias identificadas durante una auditoría.

Ingeniería de Software: Disciplina orientada al diseño, documentación y creación de soluciones informáticas bajo metodologías formales.

Ingeniería Social: Técnicas que buscan manipular a personas para obtener información o accesos no autorizados.

ISO/IEC 27001: Norma internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).

ISO/IEC 27002: Norma complementaria a la ISO 27001 que detalla controles de seguridad.

Llave FIDO2: Dispositivo físico que permite autenticación segura sin contraseña.

MFA (Autenticación Multifactor): Mecanismo que requiere dos o más factores para verificar la identidad de un usuario.

Mejora Continua (PDCA): Metodología Plan-Do-Check-Act utilizada para optimizar procesos de manera iterativa.

Normativa Interna: Conjunto de reglas y políticas establecidas por la organización.

Política de Contraseñas: Documento que establece las reglas mínimas para el uso y creación de claves seguras.

Procedimiento Normativo: Documento formal que define paso a paso cómo se ejecuta un proceso.

Redes de Computadores: Área que estudia las comunicaciones y estructuras que conectan dispositivos dentro de una organización.

Revisión Interna: Evaluación realizada por la organización para verificar el cumplimiento de controles y procesos.

Riesgo de Accesos Indebidos: Amenaza asociada a cuentas o credenciales vulnerables, inactivas o mal gestionadas.

SGSI (Sistema de Gestión de Seguridad de la Información): Marco de gestión que organiza políticas, procedimientos y controles para proteger la información corporativa.

Sincronización: Proceso mediante el cual se mantienen actualizados los datos de usuarios entre AD y servicios de la nube como Entra ID.

Taller de Ingeniería de Software: Asignatura orientada a desarrollar habilidades comunicacionales y de levantamiento de información bajo un enfoque profesional.

Trazabilidad: Capacidad de registrar y seguir el estado, evolución y acciones asociadas a una identidad o proceso.