INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE OCCIDENTE

Departamento de Electrónica, Sistemas e Informática

Desarrollo Tecnológico y Generación de Riqueza Sustentable

PROYECTO DE APLICACIÓN PROFESIONAL (PAP)

PAP4N01A, 4N01 - VINCULACIÓN CON EMPRESAS TECNOLÓGICAS I,

OPTIMIZACIÓN DE OPERACIONES DE CIBERSEGURIDAD MEDIANTE PLATAFORMAS SIEM Y XDR EN UN SOC EMPRESARIAL EN LA EMPRESA AVERTIUM

PRESENTA

Alumno: JUAN PABLO LOMELIN URIARTE

Profesor PAP: Mtro. Andrés Ruiz Sahagún

Tlaquepaque, Jalisco, 14 de mayo de 2026.

Tabla de contenido

Resumen

Capítulo 1. Introducción

En este capítulo se presenta el contexto general del proyecto PAP realizado en la empresa Avertium, enfocado en operaciones de ciberseguridad dentro de un Security Operations Center (SOC). Se describen los antecedentes de la organización, la justificación del proyecto, los objetivos de aprendizaje, las competencias a desarrollar y los entregables esperados. También se abordan los involucrados, las restricciones del proyecto y los criterios utilizados para medir el éxito del trabajo realizado.

Capítulo 2. Desarrollo del Proyecto PAP

Este capítulo describe la metodología utilizada durante el desarrollo del proyecto, basada en enfoques ágiles y prácticas de ciberseguridad. Se detallan las herramientas empleadas, como plataformas SIEM y XDR, así como las actividades realizadas dentro del SOC, incluyendo análisis de alertas, ajuste de reglas, documentación técnica y mantenimiento de infraestructura de seguridad. Además, se presentan los planes de trabajo, comunicación, calidad y seguimiento utilizados durante la ejecución del proyecto.

Capítulo 3. Reflexiones del Alumno

En este capítulo se exponen los aprendizajes obtenidos a nivel profesional, personal, social y ético a lo largo de la experiencia PAP. Se analizan las habilidades técnicas y de comunicación desarrolladas, así como la importancia del trabajo en equipo, la mejora continua y la responsabilidad en el manejo de información sensible dentro del ámbito de la ciberseguridad.

Capítulo 4. Conclusiones

En este apartado final se presentan las conclusiones generales derivadas del proyecto, destacando el impacto de la experiencia en el crecimiento profesional del estudiante y en su formación dentro del área de ciberseguridad defensiva. Asimismo, se reflexiona sobre la importancia del aprendizaje continuo, el uso de tecnologías SIEM/XDR y las oportunidades de desarrollo dentro de la industria de la ciberseguridad.

1. Introducción

La ciberseguridad representa un elemento esencial para toda organización que busca resguardar sus activos digitales. A medida que aumenta la complejidad de los ataques cibernéticos, se hace necesario contar con especialistas que identifiquen y mitiguen riesgos de forma proactiva. En este contexto, la empresa Avertium ofrece servicios completos de protección y cumplimiento normativo, con énfasis en la detección, análisis y respuesta a amenazas. El presente Proyecto de Aplicación Profesional (PAP) se desarrolla en el Security Operations Center (SOC) de Avertium y tiene como objetivo que el estudiante adquiera experiencia real en la defensa de entornos tecnológicos empresariales.

1.1 Antecedentes

Avertium es una compañía de ciberseguridad fundada en 2019 en Arizona, Estados Unidos. Su misión consiste en proteger de manera implacable a sus clientes contra riesgos cibernéticos, a través de servicios especializados en evaluación de seguridad, detección y respuesta gestionada (MXDR), así como asesoría en cumplimiento normativo (GRC). Entre sus principales soluciones se encuentran plataformas de monitoreo y análisis (SIEM, por sus siglas en inglés, y XDR, por sus siglas en inglés) que incluyen herramientas como Microsoft Sentinel, Microsoft Defender for Endpoint y otros sistemas de seguridad reconocidos en el mercado.

En 2024, Avertium expandió sus operaciones a Guadalajara, México, con el objetivo de fortalecer su presencia en América Latina. Este crecimiento implica la incorporación de talento local, lo que permite a la empresa brindar un servicio más cercano a organizaciones de la región. El PAP que se describe en este capítulo se enmarca en la necesidad de formar profesionales especializados en ciberdefensa, capaces de operar y optimizar las plataformas de seguridad gestionada.

El proyecto lleva por nombre interno "Investigación y Detección de Amenazas utilizando herramientas de seguridad de análisis y monitoreo". El puesto asignado al estudiante es el de Ingeniero interno de ciberseguridad, con la responsabilidad de aprender procesos, metodologías y herramientas que permiten la protección activa de los sistemas de los clientes. Además, se busca que el estudiante logre la certificación AZ-500, la cual avala competencias clave en la suite de defensa de Microsoft.

1.2 Justificación

La necesidad de profundizar en ciberseguridad obedece al constante crecimiento y sofisticación de las amenazas digitales, las cuales pueden ocasionar pérdidas económicas, daño reputacional y compromisos de información confidencial. Para el estudiante, participar en este PAP representa una oportunidad de experimentar la ciberseguridad defensiva en un entorno real, adquirir conocimientos prácticos y determinar futuras áreas de especialización dentro de la seguridad de la información. El alumno va a dedicar 20 horas semanales al proyecto PAP en Avertium, repartido 5 días a la semana por un periodo de 6 meses. En la semana se va a dedicar un total de 8 horas para el reporte PAP y documentación necesaria.

Por otro lado, la organización se beneficia al contar con un recurso que, además de apoyar en la solución de tickets y tareas de ingeniería, se integrará a la base de conocimientos del equipo. Esta integración es especialmente relevante en el mercado mexicano, donde el dominio del idioma y la cercanía cultural favorecen la atención de clientes locales. Con la participación del estudiante, el equipo de Avertium aspira a optimizar la distribución de cargas de trabajo y robustecer la capacidad de respuesta ante incidentes.

1.3 Objetivos de Aprendizaje

El objetivo principal es que el alumno desarrolle habilidades para manejar diferentes ecosistemas de seguridad, en general tiene que ser capaz de poder observar datos y sacar conclusiones que expliquen porque sucedió un evento u otro y posteriormente poder plantear una solución, así como implementarla.

El proyecto busca que el estudiante desarrolle competencias en tres ámbitos:

- Competencias Técnicas:
    - Manejar plataformas de seguridad como SIEM (Microsoft Sentinel) y XDR (Microsoft Defender).
    - Comprender la correlación de eventos y alertas de ciberseguridad para proponer soluciones efectivas.
    - Obtener la certificación AZ-500, que avala el conocimiento básico en la suite de defensa de Microsoft.
- Competencias Personales:
    - Desarrollar la capacidad de aprendizaje autónomo y la mentalidad de mejora continua.
    - Fortalecer la comunicación efectiva con superiores, compañeros y áreas involucradas.

- Administrar el tiempo de forma eficiente para atender tareas prácticas y labores de documentación.

- Competencias de Integración Organizacional:
  - Comprender y adoptar la cultura de ciberseguridad de Avertium, con énfasis en la colaboración y la transparencia.
  - Participar en reuniones y proyectos del SOC para alinear objetivos y mejorar la gestión de incidentes.

1.4 Inventario de competencias

INVENTARIO DE COMPETENCIAS

No.	Competencia	Tipo de competencia	Requerido	Actual	Diferencia	Prioridad
1	Competencias Técnicas del puesto					Alta
1.1	Gestión/Personalización de portales de ciberseguridad (ejemp. Microsoft Defender 365, Sentinel, USMA)	Técnica	3	1	2	
1.2	Respuesta/Resolución de tickets de clientes	Técnica	2	0	2	
2	Competencias de Integración a la Organización					Media
2.1	Capacidad de trabajar en Equipos SCRUM	Organizacional	2	0	2	
2.2	Comunicación efectiva oral y escrita en inglés y español	Organizacional	3	2	1	
3	Competencias de Desempeño Personal					Alta
3.1	Aprendizaje continuo funciones avanzadas y posibles automatizaciones	Personal	2	1	1	

NOTA: Diferencia = Requerido - Actual, donde Requerido >= Actual

Calendario de Actividades Educativas PAP

#	Actividad educatica	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**Competencias Técnicas del puesto**					x	x	x	x	x	x	x	x	x	x	x	x	x	x
1.1	Cursos Microsoft Learn/Udemy									x	x	x	x	x	x				
1.2	Curso Sentinel ONE															x	x	x	x
1.3	Sesiones de shadowing a ingenieros de mayor nivel					x	x	x	x										
1.4	Respuesta/Resolución de tickets de clientes							x	x		x		x		x		x		x
2	**Competencias de integración a la Organización**	x	x	x	x	x	x	x	x										
	Cursos Internos	x	x	x	x														
2.1	Aprender la estrategia de trabajo en equipo SCRUM de la empresa					x	x	x	x										
3	**Competencias de Desempeño Personal**																	x	x
3.1	Aprendizaje continuo funciones avanzadas y posibles automatizaciones																	x	x

1.5 Contexto interno

El proyecto PAP se desarrolla en el área de Security Operations Center (SOC) de Avertium, dedicada a la supervisión y respuesta a incidentes de ciberseguridad. En esta área confluyen especialistas en análisis de amenazas, gestión de plataformas de seguridad y atención a clientes de diversos sectores.

Los roles y puestos que participan activamente en el proyecto incluyen:

- Security Operations Manager: Supervisa el desempeño del centro de operaciones y valida el cumplimiento de las metas.
- Microsoft Product Manager: Asegura la integración y aprovechamiento óptimo de las herramientas de Microsoft.
- Cybersecurity Team Leads: Proporcionan mentoría técnica, revisan tareas y guían la evolución del estudiante.

Los principales beneficiarios de los resultados son los equipos internos de TI de los clientes, que reciben un servicio de monitoreo y protección constante, así como el propio SOC, que refuerza su capacidad de respuesta al documentar y compartir las buenas prácticas obtenidas durante la experiencia del estudiante.

1.6 Entregables

Los entregables se concentran en la documentación sistemática de los procesos y soluciones implementadas. Por un lado, se espera que cada ticket atendido incluya un registro detallado de los pasos seguidos para resolver la incidencia y las herramientas empleadas. Por otro, se contempla la elaboración de guías o manuales de referencia en la base de conocimientos interna, especialmente cuando se presenten configuraciones aplicables a múltiples clientes. Esto permitirá reutilizar el aprendizaje y optimizar el tiempo de respuesta en incidentes futuros.

1.7 Involucrados

- Dueño/patrocinador del Proyecto: Valida los resultados generales y da seguimiento a las metas propuestas durante todo el periodo de prácticas.
- Líder o responsable del proyecto: Revisa y avala las metas técnicas, incluyendo la obtención de certificaciones.
- Alumno PAP: Cumple con los objetivos de aprendizaje y aporta en la operación diaria del SOC.
- Equipo participante: Forma parte del centro de operaciones de ciberseguridad y colabora en el desarrollo de proyectos y resolución de incidentes.

- Clientes del proyecto: Organizaciones externas que se benefician de la protección y el monitoreo continuo de sus infraestructuras.

1.8 Supuestos y Restricciones del Proyecto Individual

Se parte del supuesto de que Avertium brindará el acceso y la formación necesaria para que el estudiante realice sus funciones, incluyendo cursos internos y la preparación para la certificación AZ-500. Además, se supone que habrá sesiones de acompañamiento (shadowing) con ingenieros especializados para reforzar la curva de aprendizaje.

Las restricciones principales incluyen la disponibilidad de tiempo del estudiante, quien debe equilibrar las horas de práctica con otras responsabilidades académicas y personales. Además, se considera la limitación de transporte público, que podría afectar la asistencia presencial en caso de requerirse. Pese a ello, se prevé la modalidad de trabajo híbrido y el uso de plataformas de comunicación a distancia.

1.9 Criterios de Éxito del Proyecto Individual.

El éxito del proyecto se medirá con base en la obtención de la certificación AZ-500 y en la capacidad del estudiante para resolver de forma autónoma tickets de complejidad media. También se considerará el nivel de contribución al repositorio de conocimiento interno a través de la documentación de procedimientos y mejores prácticas. De igual forma, se evaluará la integración del estudiante al equipo, reflejada en una comunicación efectiva y en la adopción de la cultura organizacional de ciberseguridad.

2. Desarrollo del Proyecto PAP

2.1 Tipo de proyecto

- Ciclo de vida del proyecto: Iterativo (Scrum/Agile - metodología ágil con sprints cortos), con sprints de 2-4 semanas.
- Características clave:
    - Proyecto tecnológico de ciberseguridad, orientado a detección y respuesta ante amenazas.
    - Uso de herramientas SIEM (Security Information and Event Management – Gestión de Información y Eventos de Seguridad) como Microsoft Sentinel y USMA, y XDR (Extended Detection and Response – Detección y Respuesta Extendida) como Microsoft Defender y Sentinel ONE
    - Cumplimiento de estándares como NIST Cybersecurity Framework (Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología de EE.UU.) y MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge – Tácticas, Técnicas y Conocimientos Comunes de Adversarios).

2.2 Administración del Proyecto

- Metodología utilizada: Agile (metodología ágil) con elementos Scrum.
- Fases:
    - Inicio: Definición de alcance, asignación de roles y acceso a herramientas.
    - Planificación: Creación de backlog (lista priorizada de tareas), priorización de tickets y diseño de sprints.
    - Ejecución: Desarrollo de actividades (monitoreo, análisis de alertas, resolución de tickets).
    - Seguimiento y control: Reuniones diarias y revisiones de sprint semanal.
    - Cierre: Documentación de lecciones aprendidas y entrega de certificación AZ-500 (Microsoft Security Operations Analyst).

2.3 Sustento Teórico y Metodológico

- Fundamento teórico:
    - Marcos de referencia: NIST CSF (Cybersecurity Framework), MITRE ATT&CK.
    - Teorías de análisis de riesgos y gestión de incidentes.
- Metodología:
    - Agile/Scrum: Sprints enfocados en prioridades del SOC (Security Operations Center – Centro de Operaciones de Seguridad).

    - Técnicas específicas: Threat hunting (búsqueda activa de amenazas), respuesta a incidentes, análisis de TTPs (Tácticas, Técnicas y Procedimientos).
- Herramientas:
    - Microsoft Sentinel (SIEM), Microsoft Defender for Endpoint (XDR), Azure Active Directory.

2.4 Descripción del Proyecto

El proyecto se centra en la optimización de plataformas de seguridad (SIEM/XDR) y el mantenimiento de la infraestructura técnica del SOC de Avertium. Como ingeniero, tu contribución principal incluye:

- Configuración de reglas de exclusión para reducir falsos positivos en alertas.
- Afinamiento de parámetros en herramientas como Microsoft Sentinel (SIEM) y Defender (XDR).
- Mantenimiento preventivo de la infraestructura de seguridad (actualizaciones, parches, integraciones).
- Documentación técnica de procesos y clientes.

Entregables:

- Reglas de exclusión: Configuraciones para reducción de ruido en el SOC, se incluye documentación den la KB (Knowledge Base – Base de Conocimiento) de la empresa.
- Evidencias en tickets: Capturas de pantalla, logs o scripts adjuntos en tickets de ServiceNow/Jira (aplicaciones de gestión de incidencias y proyectos, respectivamente).
- Guía AZ-500: Documento con resúmenes de temas clave y prácticas para la certificación.

2.5 Plan de Trabajo

No.	Actividad	Inicio	Fin
1	Curso sobre el contexto de la empresa	28/01/2026	04/02/2026
2	Shadow a ingenieros	04/02/2026	18/02/2026
2.1	Shadow a analistas	18/02/2026	02/03/2026
3	Resolución de tickets de salud en USM	02/03/2026	16/03/2026
3.1	Resolución de tickets de salud en Microsoft Sentinel	16/03/2026	30/03/2026
3.2	Resolución de tickets de salud en LogRhythm	30/03/2026	13/04/2026
3.3	Resolución de tickets de salud en Sentinel ONE	13/04/2026	27/04/2026
4	Diseño de exclusiones para Microsoft Sentinel	27/04/2026	10/05/2026
4.1	Tuneo de alarmas en USM	10/05/2026	24/05/2026
5	Resolución de tickets avanzados con asistencia de ingenieros	24/05/2026	31/05/2026

Figura 1. Plan de actividades del proyecto PAP

Figura 2. Plan de Actividades Educativas para el Desarrollo de Competencias

2.6 Equipo de Trabajo

Rol	Responsabilidad
SOC Manager	Supervisión general del proyecto y asignación de recursos.
Lead Engineer	Mentoría técnica y revisión de entregables.
Ingeniero SOC de Ciberseguridad Interno	Resolución de tickets, documentación y análisis.
Ingeniero SOC de Ciberseguridad nivel uno/dos	Resolución de tickets avanzados, juntas de resolución con los clientes.

2.7 Plan de Comunicaciones

Emisor	*Mensaje*	*Receptor*	*Medio*	*Frecuencia*
Equipo SOC	*Reporte diario de alertas*	*Clientes*	*Plataforma SIEM*	*Semanal*
Estudiante PAP	*Avance de certificación*	*Líder técnico*	*Reunión virtual*	*Semanal*
SOC Manager	*Revisión de sprint*	*Equipo completo*	*Presencial/Virtual*	*Cada 2 semanas*

Figura 3. Plan de comunicaciones del proyecto

2.8 Plan de Calidad

Emisor: *Quién Entrega*	*Entregable:* *Qué Entrega (SubEntregable)*	*Receptor:* *Quién recibe o Inspecciona*	*Criterios:* *Condiciones de Aceptación*	*Siguiente paso.* *Donde va Cuando se Autoriza.*
Estudiante PAP	*Reporte de incidente*	*Team Lead*	*Cumplimiento de SLA y NIST CSF*	*Aprobación para KB (knowledge base)*
Analista SOC	*Análisis de TTPs*	*SOC Manager*	*Alineación con MITRE ATT&CK*	*Integración a playbook*
Ingeniero SOC	*Tickets con solución al problema*	*SOC Manager*	*Alineación con MITRE ATT&CK*	*Tuneo de SIEM*

Figura 4. Plan de Calidad del Proyecto PAP

2.9 Seguimiento y Control

El monitoreo del proyecto se realiza mediante reuniones diarias con el líder técnico, donde se revisa el avance en tareas como la implementación de reglas de exclusión o ajustes en SIEM/XDR. Cada viernes, en una revisión semanal, se evalúa el cumplimiento de hitos (ej: integraciones de clientes) y la calidad de las evidencias en tickets. Si hay retrasos (ej: cambios no planificados en requisitos de un cliente), se priorizan tareas o se ajustan plazos, documentando las causas en el sistema de gestión.

En las sesiones de retroalimentación mensuales con la Coordinación PAP, se validan competencias adquiridas y se ajusta el plan de estudio si hay desviaciones (ej: ampliar tiempo en temas complejos de KQL). Los cambios significativos en el cronograma del

PAP (ej: extensión de fechas por capacitación adicional) se comunican formalmente vía correo electrónico a ambas partes.

3. Reflexiones del alumno

3.1 Aprendizajes Profesionales

Durante el desarrollo del PAP, adquirí importantes competencias que fortalecen mi perfil profesional:

La experiencia me permitió mejorar mi capacidad para comunicarme en inglés, tanto en mensajes escritos como en llamadas, abordando temas técnicos de forma natural. Además, aprendí la importancia de pedir ayuda cuando era necesario, lo que me ayudó a profundizar en procesos y técnicas específicas. Finalmente, se afianzó en mí la idea de que en el ámbito de la ciberseguridad el aprendizaje es constante y que es indispensable actualizarse continuamente.

3.2 Aprendizajes Sociales

El proyecto PAP aportó a la sociedad al desarrollar soluciones que mejoran la capacidad de reacción ante incidentes cibernéticos. Asimismo, la experiencia favoreció la creación de un ambiente colaborativo, en el que la cooperación entre compañeros y la formación continua se tradujeron en una mayor eficiencia y calidad en la atención a los clientes.

3.3 Aprendizajes Éticos

El manejo de información sensible en la infraestructura de clientes me enseñó el valor de la ética profesional. Comprendí que la confianza depositada en la correcta administración de datos es esencial para mantener relaciones sólidas y responsables. Este aspecto ético se vio reforzado en cada decisión que implicaba la gestión de datos críticos, reafirmando la importancia de actuar con integridad y profesionalismo.

3.4 Aprendizajes Personales

La experiencia en el PAP me permitió darme cuenta de que el campo de la ciberseguridad es mucho más amplio y complejo de lo que inicialmente creía. Al concluir la carrera, tenía la falsa noción de dominar completamente el área, pero trabajar dentro de un SOC me mostró la profundidad de sus diversas ramas y la necesidad de seguir aprendiendo. Este proceso me impulsó a replantear mi conocimiento y a reconocer la importancia de la formación continua.

3.5 Tareas Aprendidas

Entre las tareas que contribuyeron de forma significativa al éxito del proyecto, destaco:

- La aceptación de la colaboración de los compañeros, lo que me permitió aprender de su experiencia y enriquecer mi propio conocimiento.
- La adopción de una mentalidad proactiva, en la que siempre se buscaba mejorar lo realizado, más allá de cumplir con las tareas asignadas.

La constante búsqueda de oportunidades para optimizar procesos y proponer nuevas soluciones que incrementaran la eficiencia del SOC.

3.6 Desarrollo profesional

Esta experiencia marcó mi entrada formal en el mundo laboral de la ciberseguridad. Como interno, inicié mi trayectoria profesional en un entorno real y desafiante, lo que me impulsó a crear y fortalecer mi perfil en LinkedIn, aumentando mi red de contactos en el sector. Este primer paso ha sido fundamental para abrirme puertas en una industria en crecimiento, tanto a nivel nacional como internacional.

4. Resultados del Trabajo Profesional

4.1 Aprendizajes Profesionales

El proyecto llevado a cabo en Avertium generó resultados concretos que fortalecieron las operaciones del SOC. La implementación de reglas de exclusión y el afinamiento de parámetros en plataformas como Microsoft Sentinel y Microsoft Defender permitieron reducir de manera significativa el número de falsos positivos, optimizando el flujo de trabajo del equipo. Asimismo, la documentación generada en la Knowledge Base interna representa un activo profesional tangible que queda disponible para futuros ingenieros, mejorando la capacidad de respuesta ante incidentes similares.

4.2 Aprendizajes Sociales

El proyecto aportó valor social al reforzar la capacidad de protección de las organizaciones clientes de Avertium, muchas de las cuales dependen de la continuidad de sus operaciones digitales para brindar servicios a terceros. Al contribuir a un entorno de trabajo más colaborativo dentro del SOC, el proyecto también promovió una cultura de intercambio de conocimiento entre los ingenieros del equipo, lo que se tradujo en una atención más eficiente y coordinada hacia los clientes.

4.3 Aprendizajes Éticos

El manejo responsable de información sensible perteneciente a los clientes de Avertium fue un eje transversal del proyecto. Todas las configuraciones, análisis y documentos generados se desarrollaron bajo estrictos criterios de confidencialidad y cumplimiento normativo, alineados con marcos como el NIST Cybersecurity

Framework. El proyecto demostró que es posible alcanzar resultados técnicos sólidos sin comprometer la integridad de los datos ni la confianza depositada por los clientes.

4.4 Aprendizajes Personales

El proyecto evidenció que incorporar a un estudiante en formación dentro de un SOC real es una estrategia viable y productiva para la empresa. Los entregables generados desde tickets documentados hasta guías técnicas, demostraron que una curva de aprendizaje bien estructurada puede traducirse en contribuciones reales desde etapas tempranas. Esto reafirma el valor de programas como el PAP tanto para el alumno como para la organización anfitriona.

4.5 Aprendizajes Personales

Las tareas que mayor impacto tuvieron en los resultados del proyecto fueron:

- La configuración de reglas de exclusión en el SIEM, que permitió reducir el ruido operativo y enfocar los esfuerzos del equipo en amenazas reales.
- El mantenimiento preventivo de la infraestructura de seguridad, incluyendo actualizaciones e integraciones de nuevos clientes, que garantizó la continuidad y estabilidad del servicio.
- La elaboración de documentación técnica estructurada en la Knowledge Base, que facilitó la estandarización de procesos y la reutilización del conocimiento generado durante el proyecto.

El proyecto PAP se integró de manera efectiva al ciclo operativo de Avertium, alineándose con las metodologías ágiles (Scrum) y los estándares de calidad del SOC. La participación en sprints, reuniones diarias y revisiones semanales permitió que el trabajo realizado respondiera a las necesidades reales del equipo en tiempo y forma. Este esquema de trabajo demostró que la colaboración entre la academia y la industria puede generar resultados profesionales de alto valor, contribuyendo al crecimiento de la empresa en el mercado mexicano de ciberseguridad.

5. Conclusiones

Este PAP marcó el punto de partida formal de mi trayectoria en ciberseguridad, con énfasis en el área defensiva, y me brindó la oportunidad de ganar experiencia tangible en la salvaguarda de infraestructuras críticas. Durante esta etapa, desarrollé la capacidad de construir defensas sólidas en un entorno en permanente cambio, empleando herramientas y plataformas especializadas como SIEM y XDR. El desafío de

adaptarme a diferentes tecnologías y ambientes me evidenció cuán esencial es mantenerse en un proceso continuo de aprendizaje.

Del mismo modo, este proyecto despertó en mí el interés por explorar la vertiente ofensiva de la ciberseguridad, con el propósito de enriquecer mis competencias defensivas y contribuir con soluciones más completas. Haber formado parte de una de las pocas empresas especializadas en este campo en México me permitió dimensionar el potencial del sector y las oportunidades que ofrece un mercado aún por consolidar.

En definitiva, el PAP no solo satisfizo los objetivos contractuales y académicos establecidos, sino que se convirtió en un cimiento esencial para mi crecimiento tanto personal como profesional, reafirmando la importancia de la superación constante en una disciplina tan dinámica y exigente.