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)

ITESO, Universidad Jesuita de Guadalajara

PAP4N01B, 4N01 - VINCULACIÓN CON EMPRESAS TECNOLÓGICAS II,

AVERTIUM

PRESENTA

Alumno: ICS, RAÚL ANDRÉS VILLALPANDO BARBA

Profesor PAP: Mtro. Juan Manuel Islas Espinoza

Tlaquepaque, Jalisco, Julio 2025.

ÍNDICE

Contenido

REPORTE PAP

Presentación Institucional de los Proyectos de Aplicación Profesional

Los Proyectos de Aplicación Profesional (PAP) son una modalidad educativa del ITESO en la que el estudiante aplica sus saberes y competencias socio-profesionales para el desarrollo de un proyecto que plantea soluciones a problemas de entornos reales. Su espíritu está dirigido para que el estudiante ejerza su profesión mediante una perspectiva ética y socialmente responsable.

A través de las actividades realizadas en el PAP, se acreditan el servicio social y la opción terminal. Así, en este reporte se documentan las actividades que tuvieron lugar durante el desarrollo del proyecto, sus incidencias en el entorno, y las reflexiones y aprendizajes profesionales que el estudiante desarrolló en el transcurso de su labor.

Resumen

El presente Proyecto de Aplicación Profesional (PAP) lo realice en colaboración con Avertium, empresa especializada en ciberseguridad, cuyo objetivo es que apoye en las tareas de ingeniería que surgen en un entorno profesional, aplicando conocimientos teóricos para la detección y mitigación de amenazas cibernéticas en un Security Operations Center (SOC). Este proyecto responde a la creciente necesidad de formar profesionales competentes en el manejo de tecnologías avanzadas de seguridad, desarrollando al mismo tiempo competencias técnicas, personales y organizacionales.

La importancia de la ciberseguridad radica en la protección efectiva de los activos digitales frente a ataques cada vez más complejos. Avertium, establecida en Estados Unidos y recientemente expandida a México, ofrece servicios completos en evaluación, detección y respuesta gestionada, destacando herramientas avanzadas como SIEMS (Sistema de Gestión de Información y Eventos de Seguridad) y EDR (Detección y Respuesta de Puntos Finales). Participaré como ingeniero interno en ciberseguridad, enfocándome en optimizar procesos del SOC y buscando obtener la certificación SC-200 de Microsoft.

Este proyecto se justifica por la necesidad creciente de profesionales especializados debido al incremento y sofisticación de amenazas digitales. Dedicaré veinte horas semanales durante tres meses a la práctica profesional, combinando tareas prácticas con documentación educativa.

1. Introducción

Durante la etapa anterior de mi Proyecto de Aplicación Profesional (PAP), participé en el Security Operations Center (SOC) de la empresa Avertium, donde me enfoqué en tareas de monitoreo, análisis de alertas y generación de reportes de seguridad. En ese periodo, trabajé en un entorno altamente colaborativo, guiado por ingenieros senior, lo que me permitió familiarizarme con las herramientas y procesos clave en la defensa de infraestructuras tecnológicas empresariales.

En esta nueva fase del PAP, continuaré colaborando con Avertium, pero asumiré mayores responsabilidades como ingeniero principal para ciertos clientes. Me encargaré de liderar la comunicación directa de las noticias o dudas relacionadas con ingenieria, incluyendo llamadas periódicas y sesiones de revisión de incidentes y recomendaciones. Este nuevo rol fortalecerá mis habilidades técnicas, de comunicación y de gestión, permitiéndome aportar valor estratégico en la protección de los entornos tecnológicos asignados.

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 soluciones como Microsoft Sentinel, LogRythm 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 describo 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 "Análisis y Optimización de Procesos Técnicos en un Centro de Operaciones de Seguridad". El puesto que se me asignó 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 logre la certificación SC-200, 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 mí, 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. Voy a dedicar 20 horas semanales al proyecto PAP en Avertium, repartido 5 días a la semana por un periodo de 3 meses. En la semana voy a dedicar un total de 6 horas para el reporte PAP y documentación necesaria.

Por otro lado, la organización se beneficia al contar con un recurso que, apoyará en la solución de tickets y tareas de ingeniería, así como integrar documentación a la base de conocimientos del equipo. Con mi participación, el equipo de Avertium aspira a optimizar la distribución de cargas de trabajo y robustecer la capacidad de respuesta ante incidentes. Mi colaboración con el equipo reulta relevante en el mercado mexicano, donde mi dominio del idioma y la cercanía cultural favorecen la atención de clientes locales cuando los haya.

Objetivos

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

El proyecto busca que desarrolle competencias en tres ámbitos:

- Competencias Técnicas:
    - Manejar plataformas de seguridad como SIEM y EDR (Microsoft Defender).
    - Comprender la correlación de eventos y alertas de ciberseguridad para proponer soluciones efectivas.
    - Obtener la certificación SC-200, 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 clientes, 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.

1.3 Contexto

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.
- Advanced Detection Analyst: Asegura el aprovechamiento óptimo de las reglas de detección y generación de nuevas.
- Engineering 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.

1.4 Inventario de competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	Competencias Técnicas del puesto					
1.1	Gestión/Personalización de portales de ciberseguridad (ejemp. Microsoft Defender, Sentinel ONE, USMA Alien Vault Anywhere)	4	2	2	4	ALTA
1.2	Documentación de procesos que impactan a múltiples clientes	4	3	1	4	MEDIA
1.3	Respuesta/Resolución de tickets de clienes	3	2	1	3	ALTA
2	Competencias de Integración a la Organización					
2.1	Capacidad de trabajar en Equipos SCRUM	3	2	1	3	MEDIA
2.2	Comunicación efectiva oral y escrita en inglés y español	3	2	1	3	MEDIA
2.3	Capacidad de trabajar en Sprints Jira	4	2	2	3	MEDIA
3	Competencias de Desempeño Personal					
3.1	Habilidad para enseñar herramientas tecnológicas	3	2	1	2	MEDIA
3.2	Aprendizaje continuo, funciones avanzadas y detectar posibles automatizaciones	3	2	1	2	BAJA

1.5 Plan Educativo

		Mes 1 (semanas)				Mes 2 (semanas)				Mes 3 (semanas)				
	Actividad educatica	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
1	**Competencias Técnicas del puesto**					x	x	x	x	x	x	x	x	x
	Cursos Microsoft Learn/Udemy									x	x	x	x	x
	Curso Sentinel ONE													
	Sesiones de shadowing a ingenieros de mayor nivel					x	x	x	x					
	Respuesta/Resolución de tickets de clientes							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									
	Aprender la estrategia de trabajo en equipo SCRUM de la empresa					x	x	x	x					
3	**Competencias de Desempeño Personal**										x	x	x	x
	Aprendizaje continuo funciones avanzadas y posibles automatizaciones										x	x	x	x

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.
- Yo, como alumno PAP: Cumplo con los objetivos de aprendizaje y aporto 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.

2. Desarrollo del Proyecto PAP

2.1 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, mejoras, documentación y resolución de tickets).
    - Seguimiento y control: Reuniones diarias y revisiones de sprint semanal.
    - Cierre: Presentación de soluciones implementadas y documentación adicional.

2.2 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:
    - Sistema de tickets, SIEM, EDR, XDR y Base de Conocimientos.

2.3 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, mi contribución principal incluye:

- Configuración de reglas para reducir falsos positivos.
- Afinamiento de parámetros en herramientas de monitoreo (SIEM) y respuesta (EDR, XDR).

- Mantenimiento preventivo de la infraestructura de seguridad (actualizaciones y gestión del volumen de alertas).
- Análisis y respuesta a incidencias técnicas que surjan en el ambiente del cliente con las tecnologías que implementamos.
- Documentación técnica de procesos y clientes.

Entregables:

- Reglas de detección/exclusión: Configuraciones mejorar la eficiencia y calidad del SOC, se incluye documentación den la KB (Knowledge Base – Base de Conocimiento) de la empresa.
- Evidencias en tickets: Descripción de las soluciones, capturas de pantalla en las interfaces gráficas, logs o scripts adjuntos.
- Guías de procesos: Documentación con resúmenes de temas clave y procesos.

2.4 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).

2.5 Plan de Trabajo

No.	Competencia	Nivel Adquirido al Inicio	Nivel Objetivo al final PAP	Objetivo final PAP	Prior
1	Capacitacion sobre el contexto de la empresa	2	4	4	A
2	Shadow a ingenieros	2	3	3	A
3	Shadow a analistas	2	3	3	A
4	Resolución de tickets en USM	2	3	3	M
5	Resolución de tickets Microsoft Sentinel	3	4	4	M
6	Resolución de tickets en LogRythm	3	4	4	M
7	Resolución de tickets en Sentinel ONE	3	4	4	A
8	Diseño de exclusiones para Microsoft Sentinel	3	4	4	M
9	Tuneo de alarmas en Microsoft/USMA/Sentinel ONE	3	4	4	M
10	Resolución de tickets avanzados con asistencia de ingenieros	2	3	3	B

No.	Actividad Educativa	Mes 1				Mes 2				Mes 3			
		1	2	3	4	5	6	7	8	9	10	11	12
1	**Competencias Técnicas del puesto**												
1.1	Sesiones de shadowing a ingenieros de mayor nivel												
1.2	Curso Sentinel ONE												
1.3	Curso Microsoft Udemy												
1.4	Auxiliarme de el lead engineer para aprender LogRythm												
2	**Competencias de integración a la Organización**												
2.1	Trabajar tickets en equipo												
2.2	Aprender la planeación de un proyecto y el proceso de onboarding												
3	**Competencias de Desempeño Personal**												
3.1	Comunicación efectiva												
3.2	Trabajo en equipo												

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*

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*

2.9 Seguimiento y Control

El monitoreo del proyecto lo realizo 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. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

Generé los siguientes entregables que actualmente están en uso o tendrán aplicación futura en Avertium, entre clientes y en la comunidad técnica:

1. Documentación de queries personalizados para monitoreo de salud en agentes: Conjunto de consultas KQL diseñadas para evaluar el estado y desempeño de los agentes de seguridad en Microsoft Sentinel, facilitando la detección temprana de anomalías.
2. Recompilación de recursos clave para la preparación de la certificación SC-200: Paquete organizado de guías, tutoriales y ejemplos prácticos que ha sido adoptado como referencia interna por ingenieros en formación.
3. Documentación detallada en tickets de solución de casos diversos: Procesos estandarizados que documentan pasos, evidencias (capturas, logs, scripts) y recomendaciones, integradas en la base de conocimientos de ServiceNow.
4. Guía para aplicar etiquetas personalizadas en ServiceNow: Manual paso a paso que permite categorizar y priorizar tickets, mejorando la eficiencia en la gestión de solicitudes.
5. Certificado de aprobación del examen SC-200: Validación oficial de competencias en la suite de defensa de Microsoft, aportando valor al estatus de partner de Avertium y a mi perfil profesional.

3.2 Estimación del Impacto

Los entregables desarrollados han contribuido de manera integral a optimizar la operativa del SOC, fortaleciendo la detección temprana de incidentes y mejorando la formación de nuevos integrantes. La documentación y guías generadas han impulsado la estandarización de procesos, simplificando la incorporación de personal y la resolución de casos recurrentes. A su vez, el conjunto de recursos para la certificación SC-200 eleva la preparación técnica del equipo, consolidando la reputación de Avertium como partner de Microsoft y reforzando su capacidad para atraer y mantener proyectos de seguridad gestionada.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

Me integré en un ambiente laboral profesional con colaboración internacional, aprendí cómo coordinarme con equipos de distintos países y zonas horarias. A pesar de la tensión sociopolítica con Estados Unidos, observé que el sector de TI en México crece impulsado por la relocalización de inversiones y la alta demanda de talento especializado

Desarrollé la capacidad de elaborar hipótesis para incidentes y crear pruebas de concepto de soluciones, aprendí a personalizar plataformas de ciberseguridad como Microsoft Sentinel, USMA, SentinelOne y LogRhythm, incluyendo la creación de reglas de detección y exclusión, la integración de fuentes de logs y la implementación de nuevas soluciones.

4.2Aprendizajes Sociales

Observé cómo la optimización de procesos tecnológicos mejora la detección y gestión de ciberamenazas, protegiendo activos sensibles. Identifiqué que un SOC robusto trasmite mayor tranquilidad a las organizaciones, mitigando riesgos y fortaleciendo la confianza de los clientes. Contribuí al impulso de contratación de talento mexicano, demostrando que ingenieros locales pueden ofrecer resultados de alto nivel.

4.3 Aprendizajes Éticos

La confianza, la transparencia y la honestidad técnica son pilares en la ciberseguridad; sin ellos, las soluciones pierden eficacia.

La responsabilidad y la colaboración son fundamentales para garantizar la integridad de los procesos y la continuidad operativa.

4.4 Aprendizajes Personales

Confirmé que trabajar en ciberseguridad es gratificante y se alinea con mi pasión por la tecnología. Descubrí intereses comunes con profesionales del área, reforzando mi

sentido de pertenencia al campo. Comprendí la rentabilidad y variedad de especializaciones dentro de la ingeniería en ciberseguridad.

4.5 Tareas Aprendidas

- Factores que impulsaron el éxito:
    - Comunicación constante y colaboración abierta con el equipo.
    - Liderazgo constructivo de mis guías técnicos, con retroalimentación constructiva.
    - Agilidad en el estudio y apoyo técnicos oportuno.
- Oportunidades de mejora:
    - Optimizar la preparación para certificaciones, agilizando mis tiempos de estudio.
    - Aumentar la documentación preventiva antes de la ejecución de tareas.
    - Mejorar la planificación del tiempo general para equilibrar más eficientemente tareas prácticas y de documentación.

4.6 Desarrollo Profesional

Desarrollar este proyecto fortaleció mi visión sobre mi futuro profesional. A corto plazo, quiero centrarme en la optimización de procesos dentro de un SOC, incorporando inteligencia artificial que permita automatizar tareas y mejorar la capacidad de detección. Además, me interesa explorar la seguridad ofensiva para entender mejor las técnicas de los atacantes y diseñar defensas más robustas.

Entre mis áreas de mayor destreza se encuentran:

- La gestión de herramientas de ciberseguridad.
- El manejo de plataformas de colaboración, como Microsoft 365.
- La configuración de redes y sistemas.

Estos conocimientos se relacionan con sectores que muestran un crecimiento acelerado:

- La inteligencia artificial aplicada a la seguridad.
- La ciberseguridad como servicio gestionado.

- Las soluciones de redes resilientes.

Para avanzar, planeo seguir un camino de formación continua con certificaciones especializadas, proyectos personales y participación activa en comunidades profesionales. Sé que alcanzar estos objetivos requiere disciplina, estudio constante y la voluntad de adaptarme a las tendencias, donde la inteligencia artificial se consolida como un factor transformador de la defensa y la evolución de nuevas amenazas.

5. Conclusiones

Este ejercicio de documentación me ha permitido trazar un mapa claro de mi progreso profesional, identificar fortalezas, áreas de mejora y definir metas sólidas. Este proyecto me ayuda a fomentar mi pasión por la ciberseguridad en forma de divulgación académica, destacando los puntos clave ante académicos y profesionales.

El PAP no solo consolida mi conocimiento técnico, sino que también me posiciona estratégicamente para aprovechar oportunidades futuras. Soy consciente del camino que aún me queda por recorrer y valoro la posición privilegiada que ocupo: ahora, más que nunca, deseo maximizar mi impacto y contribuir activamente a la protección de la sociedad.

Este proceso me permitió también reflexionar sobre la importancia de seguir aprendiendo y adaptarme a un campo que evoluciona con rapidez. La formación continua y la disposición a asumir nuevos retos serán esenciales para consolidar mi trayectoria profesional y aportar soluciones de valor a las organizaciones con las que colabore.