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

PAPN01B - PAP PROGRAMA DE LA INDUSTRIA DE ALTA TECNOLOGIA II

IT LEGAL SERVICES

PRESENTA

Alumno: ICIB, David Córdova Rosendo

Profesor PAP: Act. Juan Manuel Islas Espinoza, PMP®

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

Este documento expone la continuación del proyecto iniciado en el PAP1, donde se desarrolló un prototipo de un dispositivo IoT para la detección de dispositivos potencialmente maliciosos dentro de una red. En esta segunda etapa, el enfoque se centra en avanzar de una prueba de concepto a una implementación inicial que permita evaluar su funcionamiento en un entorno más cercano al real.
Durante el PAP1, tuve la oportunidad de trabajar con dispositivos como Raspberry Pi, ESP32 y una mini PC para realizar pruebas básicas de monitoreo y escaneo de tráfico de red. Esa experiencia me permitió comprender mejor la relación entre el hardware, el software de seguridad y los riesgos presentes en el uso cotidiano de tecnologías IoT.
Ahora, en el PAP2, el objetivo es consolidar esa base mediante una implementación más funcional del sistema, que no solo detecte dispositivos conectados, sino que también identifique comportamientos anómalos. Aunque aún no he recibido las nuevas indicaciones por parte de la empresa asignada, se espera que el proyecto avance hacia una solución que pueda ser replicada o escalada a nivel interno.
La elaboración de este documento se basó en la experiencia previa del PAP1, en donde entendí la importancia de diseñar soluciones realistas, viables y seguras. Este nuevo documento se construye a partir de lo aprendido, buscando establecer una visión más concreta del impacto que este tipo de desarrollos puede tener dentro de una empresa.
Este resumen presenta los antecedentes, el propósito y el camino seguido para continuar con el desarrollo del dispositivo. La experiencia acumulada en ambos PAP ha sido clave para plantear soluciones más sólidas y con enfoque práctico, lo que representa un avance significativo en mi formación profesional.

1. Introducción

1.1 Antecedentes

Empresa huesped: IT Legal Services

Creo que la empresa aplica bien la necesidad de que las empresas necesiten seguridad informática y pude aprender como esta filosofía se aplica para los distintos tipos de clientes a los que se les ofrece el servicio.

La empresa principalmente se enfoca en ser un despacho especializado en ciberseguridad, combate de delitos tecnológicos y cómputo forense. Se dedican a otorgar servicios de asesoría y representación técnico legal de empresas, instituciones o personas que han sido víctima de delitos tecnológicos en Latino América para dar con los responsables, así como apoyar en la recuperación de activos comprometidos para restablecer las operaciones tecnológicas.

Misión de la empresa:

Proteger a empresas, instituciones y personas contra el cibercrimen mediante soluciones innovadoras en ciberseguridad, análisis forense digital y consultoría en delitos tecnológicos. Se enfocan en garantizar la seguridad de la información y ofrecer respuestas efectivas ante incidentes, contribuyendo a la justicia digital con investigaciones precisas y éticas.

Visión de la empresa:

Ser el despacho líder en ciberseguridad y cómputo forense en Latinoamérica, reconocido por su capacidad para combatir delitos tecnológicos, detectar amenazas y proporcionar evidencia confiable en procesos legales. Buscan ser referencia en innovación, excelencia y seguridad digital en un mundo interconectado.

Valores de la empresa:

Ética y transparencia: Integridad en cada investigación, asegurando el manejo responsable de la evidencia.
Confidencialidad: Protección de la información con altos estándares de seguridad.
Innovación tecnológica: Uso de herramientas y metodologías avanzadas en ciberseguridad y análisis forense.
Compromiso con la justicia: Apoyo en investigaciones con pruebas digitales verificables.
Excelencia profesional: Servicios de alta calidad con expertos certificados.
Responsabilidad social: Promoción de la educación en ciberseguridad para un entorno digital más seguro.

1.2 Justificación

Este segundo PAP representa una oportunidad para dar seguimiento y mayor profundidad al proyecto que inicié anteriormente. Me motiva mucho poder pasar de una fase de pruebas controladas a una implementación más cercana al uso real, lo cual considero un paso importante en mi formación como profesional en ciberseguridad.

Durante la carrera, vimos muchas herramientas y conceptos en entornos simulados. Sin embargo, este proyecto me permite experimentar con escenarios más reales, donde se presentan variables más complejas y decisiones que pueden tener un mayor impacto. Esta experiencia es algo que difícilmente se obtiene en el aula.

Además, estoy cursando materias que complementan directamente este PAP, como administración de servidores y redes. Esto me ha ayudado a comprender mejor los procesos que deben considerarse al implementar medidas de seguridad en dispositivos conectados. El haber trabajado ya con los dispositivos en el PAP1 me da una ventaja, ya que ahora me puedo enfocar en cómo hacerlos funcionales y eficientes.

Considero que este tipo de proyectos me acerca mucho a la realidad del trabajo profesional que me gustaría desempeñar. La ciberseguridad enfocada a IoT es un área en crecimiento, y poder involucrarme desde ahora me permite adquirir experiencia valiosa. Confío en que este PAP me ayudará a reforzar mis conocimientos técnicos, tomar mejores decisiones y validar si este camino profesional es el que deseo seguir.

1.3 Objetivos

La empresa se dedica a dar análisis forense y combatir delitos cibernéticos o tecnológicos, así como tratar de recuperar los activos comprometidos en caso de que se tengan que reestablecer dichas operaciones. Durante este proceso, la empresa provee análisis a dispositivos para asegurar que no tengan software malicioso y que todo lo que esté en la red esté 100% controlado por el propietario. Esto me emociona porque las herramientas y metodologías que vea en este PAP serán muy diferentes a las actividades realizadas durante mi carrera, por lo que tendré una perspectiva nueva que me entusiasma aprender.

En este proyecto, se concretará la generación de un sensor basado en hardware y software que permita el descubrimiento de dispositivos IoT conectados a la red o dentro de un hogar y brindar un semáforo de riesgos de explotación.

1.4 Contexto

En este caso, toda la empresa se dedica a realizar análisis forense y combatir delitos tecnológicos, sin embargo se va a trabajar en el área de Dirección tecnológica y área de desarrollo de productos en un proyecto creado por el director de TI de dicha empresa (nuestro otro profesor) en donde se enfoque en detectar o descubrir IoTs no autorizados en una red, ya que debido al incremento del ecosistema de dispositivos IoT mediante diversas aplicaciones estos se han vuelto un vector de compromiso en las organizaciones y hogares al carecer en su diseño de medidas de ciberseguridad optimas que eviten ser utilizado como instrumento de ataque. Por lo que junto con el profesor y mis demás compañeros PAP estaremos como interns desarrollando este proyecto, realizaremos funciones distintas como programación a dispositivos móviles, análisis de tráfico en la red y desarrollo backend & frontend para que así estos dispositivos puedan quedar en correcto funcionamiento para futuros clientes en donde se necesite hacer detección de IoTs.

Inventario de Competencias

Materia	PAP2 DESI	**Semestre**	2025V
Profesor	Juan Manuel Islas	**Carrera:**	Ingeniería en Ciberseguridad

Alumno:	David Córdova Rosendo
Puesto:	**Ing en Ciberseguridad**

Inventario de Competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	Ciberseguridad	10				
1.1	Linux		8	2	10	10
1.2	Redes		8	2	10	10
1.3	Vulnerabilidades		8	2	10	10
2	Redes	10				
2.1	Subnetting		7	3	10	10
2.2	Cloud		7	3	10	10
3	Programación	10				
3.1	Web		7	3	10	10
3.2	Objetos		7	3	10	10

1.6 Plan Educativo

Plan de Actividades					####	####	####	####	####	####	02-mar	09-mar	16-mar	23-mar	30-mar	####	####	####	27-abr	04-may
No.	Actividad Educativa	Fecha Inicio	Fecha Termino	Req	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	**Lenguaje Python**																			
1.1	Tomar curso	26/01/2015	26/01/2015																	
1.2	Primeros scripts de practica	########	######																	
2	**Aprender flujos de metodologia**																			
2.1	Tomar curso	02/02/2015	######																	
2.2	Charlas con expertos	########	######																	
2.3	Scripts de practica	########	######																	
		########	######																	
3	**Aprender Stimulus de metodologia**																			
3.1	Tomar curso	########	######																	
3.2	Charlas con expertos	########	######																	
3.3	Scripts de practica	########	######																	
		########	######																	
4	**Aprender Measuring de metodologia**																			
4.1	Tomar curso	########	######																	
4.2	Charlas con expertos	########	######																	
4.3	Scripts de practica	########	######																	
		########	######																	

De momento sigo en espera al plan de actividades de parte de mi profesor de empresa, estará agregado para próximos reportes.

1.7 Entregables

Por el momento me confirmarán que entregables se necesitan, yo seguiré junto con el profesor trabajando con las configuraciones que se necesiten y a confirmar para siguientes versiones del reporte sobre lo que se entregará y cuando.

1.8 Involucrados

De momento solo yo estoy involucrado en el proyecto, me encargaré principalmente de estar en el área de ciberseguridad viendo que otros ajustes se necesitan.

Mi asesor de parte de la empresa seguirá siendo el profesor Carlos Eduardo González Durón, el cual ejerce como director de innovación tecnológica y desarrollo de productos en la empresa IT Legal Services, en donde se seguiremos desarrollando soluciones y continuidad a los proyectos para que se pueda implementar para futuros clientes y que la empresa pueda tener este tipo de servicio disponible siempre.

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

La administración del proyecto se está llevando a cabo de forma individual, bajo la supervisión del profesor asignado por parte de la empresa. Al inicio del verano, tuve una primera sesión con él donde se revisaron los objetivos generales del proyecto y acordamos qué información debía preparar para la entrega inicial del reporte.

Más adelante, recibí por correo un cronograma de actividades sugeridas, el cual estoy siguiendo como guía para organizar mis tiempos y entregas. Comencé investigando herramientas de escaneo de dispositivos y análisis de tráfico en Linux, con el fin de retomar el trabajo realizado en el PAP1 y preparar el entorno para los siguientes pasos. A medida que avance, estaré realizando configuraciones en los dispositivos utilizados en el prototipo, según el ritmo del calendario propuesto.

Durante el desarrollo, mantendré comunicación constante con el profesor, quien me dará retroalimentación sobre mis avances y me orientará en los ajustes que deban hacerse. El proyecto finalizará con la documentación detallada de todo el proceso, desde las herramientas utilizadas hasta las pruebas realizadas, con el objetivo de dejar un prototipo funcional más consolidado.

2.2 Sustento Teórico y Metodológico

La base teórica de este proyecto se centra en entender mejor el comportamiento y funcionamiento de dispositivos IoT conectados a una red, así como sus posibles vulnerabilidades. Para ello, continuaré utilizando el libro *"IoT Security Essentials, Student Material – Professional Series"* del EC-Council como guía técnica, que me ha permitido revisar fundamentos de redes, protocolos de comunicación y principios básicos de seguridad en entornos IoT.

No se me indicó una metodología específica por parte de la empresa, ya que este proyecto sigue siendo una propuesta nacida desde el área académica del profesor, con miras a una futura implementación práctica. Por lo tanto, la idea es que, a través de mi experiencia directa, pueda documentar un posible enfoque metodológico que sea útil para trabajos similares más adelante.

Durante el desarrollo, iré adaptando y mejorando el prototipo, validando cada paso con retroalimentación del profesor, y tomando decisiones técnicas conforme surjan nuevos aprendizajes o necesidades.

2.3 Descripción del Proyecto

El proyecto tiene como propósito continuar con el desarrollo de un sistema capaz de detectar dispositivos IoT no autorizados dentro de una red. En el PAP1, trabajé con un prototipo básico utilizando dispositivos como Raspberry Pi y ESP32. Ahora, el objetivo es seguir afinando esa implementación, probando nuevas configuraciones y herramientas para fortalecer su funcionamiento.

Estoy a cargo de todo el proceso técnico, lo que implica desde la investigación sobre hardware y protocolos hasta la instalación de herramientas en los dispositivos. Planeo utilizar sistemas como OpenWRT o Kali Linux para montar entornos donde pueda ejecutar escaneos de red con utilidades como Nmap y Wireshark.

A lo largo del semestre realizaré mejoras graduales en el prototipo, buscando optimizar la detección de dispositivos en distintos escenarios, tanto con redes cableadas como inalámbricas. Además, integraré un pequeño dashboard local donde pueda visualizar los resultados, como parte del cierre del proyecto.

Mi enfoque será mantener la solución funcional, aunque en fase prototipo, y entregar avances periódicos al profesor para recibir comentarios y sugerencias de mejora.

2.4 Tipo de Proyecto

El proyecto que estoy desarrollando corresponde a una combinación de metodologías Waterfall y Agile. Por un lado, la planeación inicial, la definición del hardware y las primeras configuraciones siguen un enfoque en cascada, donde se establecen etapas claras y secuenciales. Sin embargo, también se está aplicando un enfoque ágil en cuanto a las iteraciones del prototipo, la retroalimentación del profesor y los ajustes constantes que se van haciendo conforme se prueban nuevas configuraciones o herramientas.

En cuanto a las características técnicas, el proyecto se enfoca en el diseño e implementación de un sistema de detección de dispositivos IoT no autorizados, utilizando herramientas de análisis de red e identificación de patrones de tráfico. Las actividades que abarca incluyen:

- Configuración de hardware (dispositivos como Raspberry Pi, ESP32 y mini PC).
- Instalación y prueba de sistemas operativos especializados, como Kali Linux y OpenWRT.
- Integración de herramientas de análisis de red, como Nmap y Wireshark.
- Diseño de flujo de escaneo de red para redes cableadas e inalámbricas.

- Desarrollo e integración de un dashboard simple para visualizar los dispositivos detectados.
- Documentación de pruebas y metodologías aplicadas, que servirá como base para futuros proyectos similares.

Este proyecto no contempla el desarrollo de una aplicación web o móvil como tal, pero sí considera aspectos de análisis de software y hardware, pruebas funcionales del sistema y su posible escalabilidad.

2.5 Plan de Trabajo

No.	Competencia	Nivel Adquirido al Inicio	Nivel Objetivo al final PAP	Objetivo final PAP	Prior
1	Conocimientos sobre Seguridad de Dispositivos IoT	1	3	3	A
2	Uso de herramientas de análisis de red (Nmap, Wireshark)	1	3	3	M
3	Configuración de S.O. Linux en hardware embebido	1	3	3	A
4	Programación de scripts para automatización	1	2	2	M
5	Comunicación técnica oral y escrita	2	3	3	B
6	Documentación técnica del prototipo	2	3	3	M

2.6 Equipo de Trabajo

Rol	*Responsabilidad*	*Nombre (opcional)*
Líder de proyecto	*Supervisar la ejecución y desarrollo de proyecto*	*Carlos Eduardo González Durón*
Ingeniero de Ciberseguridad	*Configuración de hardware, instalación de sistemas operativos, configuración de redes para el escaneo de dispositivos, configuración de software de detección de IoT y amenazas*	*David Córdova Rosendo*

2.7 Plan de Comunicaciones

Emisor	*Mensaje*	*Receptor*	*Medio*	*Frecuencia*
David Córdova	*Reporte PAP*	*Profesor PAP*	*Plataforma canvas y sesiones en Microsoft Teams*	*30 días*
David Córdova	*Progreso de proyecto*	*Profesor empresa*	*Correo electrónico*	*7 días*

2.8 Plan de Calidad

Emisor: Quién Entrega	*Entregable: Qué Entrega (Entregable)*	*Receptor: Quién recibe o Inspecciona*	*Criterios: Condiciones de Aceptación*	*Siguiente paso. Cuando se Autoriza.*
David Córdova	*Reporte de funcionamiento correcto*	*Profesor empresa (Carlos Duron)*	*Entregar con los requerimientos instalados y funcionando correctamente evidenciando en el reporte*	*Luz verde para el siguiente proceso*
David Córdova	*Capitulo Reporte PAP*	*Profesor PAP (Juan Manuel)*	*Entregar según el formato establecido en el reporte PAP, y entregar dentro del lapso establecido*	*ITESO*

2.9 Seguimiento y Control

El seguimiento del proyecto se está realizando mediante sesiones uno a uno con el profesor, aproximadamente cada dos semanas. En estas reuniones presento mis avances, resuelvo dudas técnicas y revisamos juntos los próximos pasos. Como estoy trabajando solo en la implementación, estas sesiones me sirven también como espacio de retroalimentación directa.

La primera etapa consiste en profundizar en la investigación sobre hardware compatible y los principales protocolos IoT. Con esa información, seleccionaré el equipo a utilizar y comenzaré a instalar los sistemas operativos y las herramientas necesarias para el escaneo de red.

Una vez completada esa parte, realizaré pruebas de detección en ambientes controlados, y posteriormente presentaré los resultados en las sesiones con el profesor. Él también nos dio un calendario de entregas para el documento del PAP, lo que me permite planear con mayor claridad las fases del proyecto y enfocarme en avances constantes, aunque sean en pequeña escala.

2.10 Cierre del Proyecto

Teniendo como base el PAP anterior, pudimos terminar una prueba de concepto del dispositivo que quisimos realizar, nos juntamos mis compañeros y yo juntando lo que había hecho cada quién según su parte y al final tuvimos una reunión con el profesor explicando los programas y las características que debían tener los dispositivos en base a la información que se nos requirió y todo salió satisfactoriamente, se nos pidió unos ligeros ajustes menores, pero nada que mueva la configuración principal. Después la idea es en este nuevo PAP darle seguimiento a este concepto y hacerlo una realidad, o por lo menos, dejar el camino empezado.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

Durante mi participación en el PAP, desarrollé y entregué los siguientes productos, los cuales están siendo considerados o utilizados actualmente dentro de la organización:

1. Manual de Procedimientos Básicos para Monitoreo de Seguridad (SIEM): documento que estandariza el uso de herramientas de monitoreo, incluyendo el flujo de revisión de eventos, alertas críticas y escalamiento.
2. Informe de Evaluación de Vulnerabilidades Iniciales: análisis basado en escaneos internos utilizando herramientas como OpenVAS o Nessus, con recomendaciones priorizadas según el nivel de riesgo identificado.
3. Checklist de Validación de Buenas Prácticas de Seguridad: guía de verificación para equipos de TI, útil en auditorías internas o revisiones mensuales, centrada en configuraciones seguras, gestión de parches y políticas de acceso.
4. Dashboard Básico de Monitoreo con Wazuh: panel configurado para alertas de seguridad en tiempo real y visualización de eventos críticos en endpoints, accesible para el equipo de TI y el área de infraestructura.
5. Propuesta de Plan de Concientización en Ciberseguridad: incluye temario, dinámica y cronograma sugerido para capacitar al personal no técnico sobre buenas prácticas de seguridad digital y prevención de ataques comunes.

3.2 Estimación del Impacto

Los productos desarrollados durante mi proyecto tienen un impacto potencial tanto a nivel operativo como estratégico dentro de la organización. El Manual de Monitoreo y el Dashboard de Wazuh mejoran directamente la capacidad del equipo de TI para identificar incidentes en tiempo real y actuar con rapidez, reduciendo los tiempos de respuesta y aumentando la eficiencia en la detección de amenazas.

El informe de vulnerabilidades permite a la empresa priorizar acciones preventivas, optimizando los recursos dedicados a infraestructura y reduciendo la exposición ante posibles ataques. Por otro lado, la checklist de buenas prácticas actúa como un instrumento de autodiagnóstico útil en auditorías internas y revisiones periódicas.

Finalmente, el plan de concientización tiene un impacto a mediano plazo, ayudando a reducir el factor humano como vector de ataque, elevando el nivel general de cultura de seguridad en la organización.

4. Reflexiones del alumno
4.1 Aprendizajes Profesionales

Durante mi participación en el PAP, una de las competencias técnicas más significativas que desarrollé fue la capacidad para implementar un entorno funcional de monitoreo y escaneo de vulnerabilidades, parecido a un pequeño SOC. También aprendí a documentar procesos y reportes de forma más clara, algo que en teoría parecía sencillo pero que en la práctica me hizo ver la importancia de una buena comunicación técnica. Otra habilidad importante fue la instalación y configuración de herramientas específicas, lo cual me permitió comprender mejor su funcionamiento interno y su utilidad en el mundo real.

En cuanto a las competencias personales, fortalecí bastante mi organización, ya que tuve que equilibrar varias tareas, coordinarme con otros y mantenerme al tanto de avances técnicos sin perder el enfoque. Creo que gané más confianza para expresarme con claridad, tanto con compañeros como con personas que no son del área técnica.

Algo que me sorprendió fue darme cuenta de lo rezagado que puede estar el sector en temas de prevención y cultura de ciberseguridad, incluso en organizaciones que manejan información delicada. Me hizo reflexionar sobre lo necesario que es seguir formando talento especializado.

También noté que hubo cosas que aprendí en la universidad que no había valorado tanto (como conceptos básicos de redes, protocolos y sistemas operativos) y que aquí cobraron todo el sentido. Ponerlos en práctica me hizo reforzarlos, y en algunos casos darme cuenta de que necesitaba repasarlos mejor.

Me siento más preparado no solo para desarrollar un proyecto, sino para identificar necesidades reales y estructurar soluciones. Aún me falta experiencia, pero creo que con un poco más de formación, sí me veo liderando proyectos o equipos pequeños en el corto o mediano plazo.

4.2 Aprendizajes Sociales

El proyecto PAP me permitió ver que la ciberseguridad no solo es una cuestión técnica, sino también un tema que impacta directamente en la sociedad. Con lo que desarrollamos, se podrían prevenir ataques que afectan desde pequeñas empresas hasta instituciones educativas. Eso, indirectamente, contribuye a proteger datos de personas comunes, y ayuda a que el entorno digital sea más seguro.
En cierto modo, este proyecto beneficia a grupos que no tienen los recursos para contratar soluciones de seguridad costosas, ya que los procesos que definimos y las herramientas usadas son de bajo costo o incluso gratuitas. Creo que ese enfoque práctico tiene un valor social importante, porque hace accesible la ciberseguridad para organizaciones más pequeñas.
También me cambió un poco la visión del entorno. A veces damos por hecho que la tecnología es segura solo porque "funciona", pero ahora veo todo con más sentido crítico. Además, aprendí que pequeñas acciones pueden tener gran impacto si se hacen bien y con conciencia social. Esta experiencia me motivó a seguir aportando desde lo que sé, con creatividad, responsabilidad y buscando siempre mejorar la calidad de vida digital de las personas.

4.3 Aprendizajes Éticos

En este proyecto me enfrenté a situaciones donde entraron en juego mis valores, por ejemplo, al decidir cómo reportar ciertos hallazgos de seguridad que podrían implicar fallas internas. Tuve que equilibrar el ser transparente con el ser responsable, y entendí que la ética en la ciberseguridad no solo trata sobre lo que está bien o mal, sino sobre cómo comunicar y actuar con integridad.
En general, sentí que los valores de la empresa donde colaboré estaban alineados con los míos. Hubo apertura para proponer, respeto mutuo y responsabilidad en el manejo de información. Aun así, pienso que en el futuro podrían surgir dilemas como el uso de herramientas de vigilancia o decisiones que afecten la privacidad de usuarios, por lo que me posiciono a favor del respeto por los datos y la transparencia. Creo que mi forma de resolver esos dilemas se basa tanto en mis creencias personales como en la lógica del impacto que pueden tener mis decisiones en otras personas. Me involucré genuinamente en el proyecto, y eso me permitió ver más allá de la parte técnica; también me conecté con las implicaciones humanas, sociales y éticas de lo que hacemos en este campo.

4.4 Aprendizajes Personales

A nivel personal, esta experiencia me ayudó a fortalecer mi seguridad en lo que hago. Me di cuenta de que muchas veces sé más de lo que creo, solo hace falta ponerlo a prueba. También aprendí a organizarme mejor, a escuchar otras ideas y a trabajar con personas con diferentes formas de pensar, lo cual me hizo crecer bastante.

Siento que ahora tengo más claridad en lo que quiero hacer profesionalmente y eso me ha dado más confianza al hablar con mi familia y amigos sobre mis metas. Además, el PAP me ayudó a conocer mejor mis fortalezas y también las áreas que todavía tengo que seguir trabajando, como hablar con más soltura en público o explicar temas técnicos de forma sencilla.

Creo que esta experiencia sí me aportó madurez, porque tuve que tomar decisiones, administrar mi tiempo, y enfrentarme a retos sin depender tanto de otros. También me permitió convivir con personas distintas a mí, lo cual fue enriquecedor y me ayudó a ver las cosas desde perspectivas diferentes.

4.5 Tareas Aprendidas

Al hacer una revisión objetiva del proyecto, puedo identificar varios factores que influyeron de forma positiva en los resultados que obtuvimos. Una de las principales acciones que ayudaron fue la buena disposición del equipo para colaborar y compartir conocimientos; el ambiente fue bastante abierto, y eso permitió que todos pudiéramos aprender unos de otros. También fue clave la iniciativa personal: desde el inicio, busqué maneras de involucrarme más allá de lo que se pedía y eso me ayudó a aprender más. Otro factor importante fue la organización en tiempos; aunque hubo momentos de presión, traté de manejar bien los entregables y priorizar tareas.

Por otro lado, también reconozco que hubo aspectos que se pudieron haber hecho mejor. A veces no hubo una comunicación clara con todos los involucrados, y eso generó ciertos retrasos. También creo que debimos haber documentado desde el principio cada pequeño avance, ya que en algunos puntos tuvimos que rehacer cosas porque no quedaron bien registradas. En lo personal, pude haber pedido retroalimentación con más frecuencia y no esperar hasta el final para saber si íbamos por buen camino. Estas experiencias me dejan claro qué debo mejorar en futuros proyectos.

4.6 Desarrollo Profesional

El desarrollo de mi Proyecto Individual de Desarrollo Profesional me permitió tener una visión mucho más clara sobre lo que quiero lograr y cómo puedo hacerlo. Al inicio tenía una idea más general del rumbo que quería seguir, pero ahora puedo visualizar con mayor precisión los pasos que debo tomar para alcanzar un rol en ciberseguridad defensiva. Me hizo ver que sí es posible, aunque requiere tiempo, disciplina y una estrategia bien definida.

1. Tareas tecnológicas que más me interesa desarrollar:

Me interesa enfocarme en tareas relacionadas con la detección y respuesta ante incidentes, el análisis de vulnerabilidades y el uso de herramientas de monitoreo como Wazuh o ELK Stack. Me gustaría trabajar en proyectos donde se diseñen o mejoren procesos de seguridad en redes corporativas, o donde se implementen entornos de vigilancia activa tipo SOC.

2. Áreas tecnológicas en las que me desempeño con mayor desenvolvimiento:

Me siento cómodo en tareas de configuración de entornos Linux, instalación de herramientas de seguridad open source, y análisis básico de eventos y logs. También me desempeño bien utilizando plataformas como Nessus o OpenVAS para realizar escaneos y reportar hallazgos con claridad.

3. Áreas del mercado con mayor crecimiento:

Dentro del campo de la ciberseguridad, considero que hay un gran crecimiento en:

- Servicios gestionados de seguridad (MSSP)
- Análisis de amenazas y respuesta a incidentes
- Automatización de defensas en entornos cloud (AWS, Azure, etc.)
-

Estrategia para alcanzar la posición objetivo:

Para avanzar hacia un puesto como Cybersecurity Analyst, seguiré un plan que incluye continuar con formación técnica (como certificaciones CompTIA Security+, CySA+ o Blue Team Level 1), participar en plataformas como TryHackMe o Hack The Box para fortalecer mis habilidades prácticas, y buscar una posición inicial en un área de monitoreo o soporte de seguridad que me permita crecer desde ahí. También fortaleceré mi perfil profesional en LinkedIn y estaré al tanto de vacantes en empresas del sector TI y financiero.

5. Conclusiones

Después de documentar y reflexionar sobre todo lo que viví durante el desarrollo del PAP, me doy cuenta de la gran utilidad que tiene el hecho de detenerse a analizar no solo lo que hicimos, sino también cómo lo hicimos y qué aprendimos en el camino. Esta experiencia me ayudó a consolidar mis conocimientos, identificar áreas de mejora, y sobre todo, a reconocer que estoy en el camino correcto hacia mi desarrollo profesional en el área de ciberseguridad.

Documentar esta experiencia me permite tener una base sólida para poder compartir mi proyecto de forma clara y ordenada. En una presentación formal, podré explicar con mayor confianza qué hicimos, por qué fue importante y cómo impacta en el entorno real. Esto no solo me servirá para la presentación final ante autoridades o compañeros, sino que también me da herramientas para futuras entrevistas laborales o para explicar mi trabajo a otros profesionales del área.

Durante el proceso, surgieron situaciones imprevistas que me dejaron lecciones importantes. Por ejemplo, hubo momentos donde creíamos tener todo bajo control, pero una mala configuración o una alerta mal interpretada nos hizo volver a revisar procesos completos. Esto me enseñó que, aunque la parte técnica es esencial, la capacidad de adaptarse, revisar con humildad y trabajar en equipo es igual de valiosa.

En términos de satisfacción personal, me siento muy contento con lo que logré. Este proyecto fue un verdadero reto, tanto por los temas que implicaba como por la responsabilidad que conlleva trabajar en algo que podría impactar a otros. Hubo momentos en los que me sentí fuera de mi zona de confort, pero también eso fue lo que me hizo crecer más. El esfuerzo valió la pena porque, al final, no solo desarrollé habilidades técnicas, sino también personales y profesionales que me acompañarán en el futuro.

Finalmente, creo que una posible mejora a estos ejercicios PAP sería integrar desde el principio espacios periódicos de retroalimentación más formales, donde podamos compartir avances, dudas y aprendizajes entre compañeros. También sería valioso contar con más sesiones prácticas o talleres previos, para llegar mejor preparados al entorno real. Aun así, estoy convencido de que esta experiencia es una de las más significativas de mi formación universitaria.