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

PAP4N01 PROGRAMA DE LA INDUSTRIA DE ALTA TECNOLOGIA I

IT LEGAL SERVICES, JARDINES DEL COUNTRY

PRESENTA

Alumno: ISI, Jonathan Rafael López Contreras

Profesor PAP: Juan Manuel Islas Espinoza, PMP®

Tlaquepaque, Jalisco, mayo de 2023.

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 proyecto PAP I enfocado a Evaluación de la ciberseguridad a la infraestructura de radiocomunicaciones de emergencia y seguridad pública del estado de Jalisco, es un PAP único en el sentido en que, si bien la obra comúnmente se hace por dinero, al estar trabajando para un cliente como lo es gobierno, tiene un impacto directa o indirectamente a la ciudadanía y su seguridad. El líder del proyecto Carlos Durón, nos guiará a través de las evaluaciones de riesgo y pruebas de penetración para la elaboración de planes de riesgo y mitigación, junto con la instalación de software de monitoreo y la elaboración de documentos y reportes profesionales.

El proyecto se enfoca a la mejora de la seguridad informática del lado de telecomunicaciones vía radio, en el departamento de Evaluaciones de Seguridad y riesgo tecnológico, me involucraré además con otros alumnos PAP, profesionistas de alta categoría los cuales nos enseñaran a realizar de forma profesional y éticamente los hackeos y pruebas, ya que uno de los impulsos más importantes de IT Legal Services es manejarse siempre con ética, honestidad, profesionalismo, objetividad e imparcialidad ante cualquier situación.

Además, me involucraré con personal del cliente, siendo seguridad pública con quien conviviré para entender la infraestructura, entender las decisiones por las cuales implementaron sus sistemas de cierta forma y a partir de ello realizar planes de riesgos con enfoque al centro.

1. Introducción

Antecedentes

El PAP que he inscrito ha sido con la empresa IT Legal Services, ellos se dedican a pruebas de penetración como lo serían páginas WEB, aplicativos móviles, videovigilancia entre otros, mejora de seguridad en redes, sistemas de dominio, comunicaciones y despacho legal de crímenes tecnológicos, entre sus clientes se encuentran diversos individuos privados sobre todo para el área legal, empresas privadas y gobierno estatal. La misión del negocio a grandes rasgos es la mejora continua de seguridad informática en ámbitos tecnológicos y legales.

1.1Justificación

El proyecto en el cual estoy participando es Evaluación de la ciberseguridad a la infraestructura de radiocomunicaciones de emergencia y seguridad pública del estado de Jalisco. Este proyecto me motiva ya que es un primer acercamiento al mundo laborar desde la perspectiva del apoyo ciudadano, mi investigación y proceso del análisis de la seguridad informática pudiera ayudar a mejorar la infraestructura pública y dejar un impacto positivo en la industria. A través de la carrera nos han enfocado a ser personas con ética y utilizar nuestro conocimiento para el bien y en pro de la sociedad, este PAP cubre esos requisitos personales míos y me entusiasma a seguir adelante.

Las horas necesarias a las semanas serían aproximadamente de 18 a 20 horas, en lo personal he asistido a competencias de hacking ético y los profesores nos capacitaron a un nivel adecuado para las evaluaciones de seguridad empresariales. Además, IT Legal Services nos apoya con capacitaciones de módulos específicos del EC Council, capacitación de como utiliza la infraestructura de comunicaciones y programas el gobierno de Jalisco. Nos permitirá conocer las instalaciones del gobierno y analizarlas de forma física.

En lo personal, esta línea de negocio me resulta bastante atractiva, hacer consultorías a diversos clientes y conocer su red me es fascinante. Es ser White hat hacker como lo establecí desde que entré a la carrera, aplicando mis conocimientos en apoyo a la sociedad.

1.2 Objetivos

El Objetivo de IT Legal Services nace originalmente de ver un hueco en la seguridad informática en el ámbito legal y ser el primer despacho en México en ofrecer servicios legales con enfoque a delitos informáticos, con el tiempo la empresa se fue expandiendo y acaparando diversas áreas de la seguridad informática. La empresa se involucra en proyectos PAP para formar a los nuevos profesionales en ciberseguridad y brindarnos apoyo laboral para hacer crecer a los profesionistas.

IT Legal Services es una empresa de renombre en múltiples áreas, espero obtener la experiencia en campo de lo que es hacer un análisis de vulnerabilidades, junto con una prueba de penetración especifica al área de radios, además de aprender cómo hacer reportes de forma profesional.

1.3 Contexto

El departamento en el trabajaré se llama Evaluaciones de Seguridad y riesgo tecnológico, en esta área nos enfocaremos a hacer evaluaciones de seguridad a múltiples dispositivos y a la mejora de esta en base a los conocimientos previos y cursos a tomar. Durante el transcurso del proyecto seremos becarios en el área.

1.4 Entregables

A lo largo del PAP se realizarán dos entregables, un Plan de mitigación de riesgos, en el cual estableceremos en base a GRC las prioridades de nuestra investigación de vulnerabilidades y pruebas de penetración. Nuestro segundo entregable sería la documentación aprendizajes logrados, en el cual estableceremos lo elaborado, desde las detecciones, métodos de resolución y sugerencias a futuro.

1.5 Involucrados

Este proyecto PAP desde mi perspectiva, a pesar de ser mi primero, es bastante único, IT Legal Servicies ha dado la oportunidad de sobrellevar un proyecto para el gobierno, cuyos interesados principalmente es seguridad pública y por ende los ciudadanos del estado de Jalisco. Nuestro proyecto podrá determinar y proteger de las vulnerabilidades actuales en su infraestructura. En mi caso el director de comunicaciones de la institución gubernamental será uno de los que aprueben el entregable, junto con el líder del PAP. Junto conmigo estará otro alumno que ha inscrito el PAP en IT Legal Services de forma directa, junto con otros 6 que estarán haciendo evaluaciones a distintas áreas.

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

La administración del proyecto PAP es bastante directa, en mi caso se inicia haciendo una evaluación inicial del centro, conociendo un poco más de su historia y su administración interna, una vez ya involucrados en los procesos, planeamos nuestra serie de reconocimiento y exploración, de esta forma podemos estar seguros y planear la siguiente fase, en la ejecución basados en la parte de planificación/exploración procedes a ejecutar las vulnerabilidades y ver su alcance, de esta forma podemos darle un seguimiento y control si seguimos avanzando en nuestra escalación de privilegios, manteniendo accesos y reportando. Cada vulnerabilidad debe de ser valorada y ver el impacto futuro al centro. La siguiente etapa entramos en la remediación de lo analizado, realizando un plan de mitigación de riesgos, priorizando y parchando, dependiendo de la gravedad. Para finalmente establecer herramientas de monitoreo y realizar los reportes necesarios y documentación adecuada.

2.2 Sustento Teórico y Metodológico

Las evaluaciones de seguridad en seguridad informática es una práctica que se ha utilizado durante mucho tiempo para mejorar la protección de los sistemas informáticos. Esta práctica se centra en encontrar y corregir vulnerabilidades en los sistemas antes de que los criminales informáticos puedan explotarlas. El hacking ético se realiza a través de una serie de pasos y procesos para asegurar la seguridad de los sistemas. Esta metodología de seguridad se compone de varias etapas, desde la identificación de la amenaza hasta el desarrollo de un plan de acción para mitigarla.

1. Identificación de la amenaza: Esta etapa se centra en identificar y analizar amenazas potenciales a los sistemas informáticos. Puede incluir la recopilación de información sobre los sistemas, los entornos de red y la forma en que se relacionan con otros sistemas, esta etapa se divide en los cinco pasos del hacking
2. Análisis de amenazas: Esta etapa implica el análisis de los datos recopilados durante la etapa de identificación de amenazas para determinar la gravedad de la amenaza. Esto puede incluir el análisis de los datos para determinar el alcance de la amenaza, el grado de riesgo y la posibilidad de desarrollar un plan de acción para mitigarla.
3. Plan de acción: Esta etapa implica el desarrollo de un plan de acción para mitigar la amenaza. El plan puede incluir la implementación de soluciones técnicas, el establecimiento de políticas de seguridad o el entrenamiento de los empleados.
4. Prueba de la solución: Esta etapa implica la evaluación de la solución para asegurarse de que funciona como se esperaba. Esto puede incluir pruebas de penetración, auditorías de seguridad y evaluaciones de vulnerabilidades.
5. Documentación: Esta etapa implica la documentación de todas las soluciones implementadas, así como un informe detallado sobre los resultados de la prueba de

la solución. Esta documentación es importante para que el personal de seguridad pueda entender cómo se implementaron las soluciones y cómo funcionan.
6. Evaluación de la seguridad: Esta etapa implica la evaluación continua de la seguridad de los sistemas para asegurarse de que están protegidos. Esto puede incluir la implementación de controles de seguridad, la realización de pruebas de penetración y la monitorización de los sistemas para detectar cambios o vulnerabilidades.

Siguiendo esta metodología, las organizaciones pueden estar seguras de que sus sistemas están protegidos contra amenazas externas. Esta metodología ofrece un marco estructurado para garantizar la seguridad de los sistemas de una organización.

Además de las seis etapas de la metodología de hacking ético descritas anteriormente, hay cinco fases principales en la metodología del hacker: preparación, inicio, explotación, mantenimiento y salida.

1. Preparación: Esta etapa se centra en la recopilación de información sobre el sistema objetivo. Esto incluye la recopilación de información sobre el sistema, la red y los usuarios asociados.
2. Inicio: Esta etapa implica la exploración del sistema para identificar posibles vulnerabilidades. Esto puede incluir el análisis de los datos recopilados durante la etapa de preparación para detectar posibles vulnerabilidades.
3. Explotación: Esta etapa se centra en la explotación de las vulnerabilidades identificadas en la etapa de inicio. Esto puede incluir la ejecución de códigos maliciosos para obtener acceso privilegiado al sistema.
4. Mantenimiento: Esta etapa se centra en la permanencia en el sistema. Esto puede incluir el uso de herramientas de seguridad para evitar ser detectado, así como la búsqueda de nuevas vulnerabilidades para aprovechar.
5. Cubrir huellas: Esta etapa implica la salida del sistema sin ser detectado. Esto incluye la limpieza de los registros de acceso para evitar que el intruso sea descubierto.

2.3 Descripción del Proyecto

En base a la teoría los entregables se basan en cada etapa del hacking ético, de esta forma podemos cubrir todo el ciclo de seguridad informática y obtener mejores resultados, mi proyecto PAP forma parte de un proyecto mayor, siendo la Evaluación De La Ciberseguridad a Seguridad Pública Del Estado De Jalisco.

En el proyecto de telecomunicaciones, detectaremos vulnerabilidades a través de diversas metodologías y programas de evaluación de seguridad, seguido se realizará el análisis de vulnerabilidades para tener una base sólida para el plan te mitigación de

riesgos. Una vez elaborado se instalará las herramientas de monitoreo para terminar con la documentación y el reporte de vulnerabilidades

En este proyecto nos basamos en la metodología de la seguridad informática y la metodología del hacker ético, son recursos bastante conocidos en la industria para lograr una evaluación completa viendo desde todos los ángulos de seguridad informática. Estas metodologías han sido perfeccionadas por años y son del dominio público. Herramientas especificas a utilizar en la parte de pentesting sería metaexploit, un framework de pentesting libre a público donde automatiza y diseña ataques.

El alcance de este proyecto sería una evaluación de seguridad, desde el punto de vista tanto del equipo de pruebas de seguridad (Red Team) como del equipo de defensa (Blue Team), en el área específica de infraestructura de radio y telecomunicaciones de emergencia. Esto permitirá a los profesionales de seguridad identificar y evaluar los riesgos de seguridad existentes, así como proporcionar recomendaciones para reforzar la seguridad de la infraestructura de radio y telecomunicaciones de emergencia, garantizando su funcionamiento adecuado, continuo y seguro.

No.	Competencia	Nivel que tiene el Alumno	Nivel Requerido PAP	Objetivo al Final del PAP	Prioridad
1	Detección e Identificación de Vulnerabilidades	1	2	2	A
2	Análisis de vulnerabilidades	1	3	2	A
3	Plan de mitigación de riesgos	0	1	1	M
4	Herramientas de monitoreo y detección de amenazas	1	2	2	M
5	Reporte de vulnerabilidades y Documentación	2	3	2	B

2.4 Plan de Trabajo

No.	Actividad	Fecha Inicio	Fecha Termino	Días de trabajo	Estado
1	Detección e Identificación de Vulnerabilidades				
1.1	Alcance del proyecto	16-ene	23-ene	2	Finalizado
1.2	Identificación de amenazas	23-ene	3-feb	4	Finalizado
1.3	Explotación de amenazas	23-ene	3-feb	4	Finalizado
2	Análisis de vulnerabilidades				
2.1	Mantenimiento de amenazas	6-feb	17-feb	4	Finalizado
2.2	Análisis de amenazas	6-feb	17-feb	4	Finalizado
3	Plan de mitigación de riesgos				
3.1	Elaboración de plan de acción	17-feb	3-mar	4	En progreso
3.2	Prioritisación de remediación y parcheo	17-feb	3-mar	4	En progreso

3.3	Aplicación de parches y actualizaciones de seguridad	17-feb	3-mar	4	En progreso
4	Herramientas de monitoreo y detección de amenazas				
4.1	Prueba de solución	6-mar	31-mar	8	Candado
4.2	Instalación y operación del sistema de monitoreo y detección de amenazas	6-mar	31-mar	8	Candado
5	Reporte de vulnerabilidades y documentación				
5.1	Cubrir huellas	1-abr	28-abr	8	Candado
5.2	Elaboración de documentación	1-abr	28-abr	8	Candado
5.3	Evaluación de seguridad	1-abr	28-abr	8	Candado

Plan de Actividades

No.	Actividad Educativa	Tipo Actividad	Prereq	Total Hrs	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Obj
1	**Detección e Identificación de Vulnerabilidades**																						
1.1	Conocimiento de la infraestructura de red y datos en radios	Curso Presencial		6	16-ene	20-ene																	
1.2	Tecnicas de identificación de dispositivos de radios	Curso Presencial	1.1	6	16-ene	20-ene																	
1.3	Escaneo de vulnerabilidades en dispositivos radios	Autoestudio/Curso	1.2	10	23-ene	27-ene																	
1.4	Identificación de vulnerabiliades	Autoestudio/Curso	1.3	6	23-ene	27-ene																	
1.5	Explotación de vulnerabilidades	Autoestudio	1.4	10	30-ene	3-feb																	
2	**Analisis de vulneravilidades**																						
2.1	Metodos de evaluación de vulnerabilidades	Curso Presencial		5	6-feb	17-feb																	
2.2	Evaluación de riesgos	Curso Presencial	2.1	5	6-feb	17-feb																	
3	**Plan de mitigación de riesgos**																						
3.1	Conocimiento básico de GRC	Autoestudio		6	6-feb	3-mar																	
3.2	Prioritisación de remedación y parcheo	Curso Presencial	3.1	6	6-feb	3-mar																	
3.3	Aplicación de parches y actualisación de seguridad	Curso Presencial	3.1	6	6-feb	3-mar																	
4	**Herramientas de monitoreo y detección de amenazas**																						
4.1	Identificación y evaluación de software de monitoreo	Autoestudio		6	6-mar	31-mar																	
4.2	Instalación y operación del sistema de monitoreo	Autoestudio	4.2	10	6-mar	31-mar																	
4.3	Instalación y operación del sistema de detección de amenazas	Autoestudio	4.2	10	6-mar	31-mar																	
5	**Reporte de vulnerabilidades y documentación**																						
5.1	Buena comunicación escrita y oral	Autoestudio		10	16-ene	28-abr																	
5.2	Conocimiento de presentaciones de reportes de seguridad	Autoestudio/Curso		9	16-ene	28-abr																	
5.3	Redacción de vulnerabilidades, documentación y planes de riesgo	Autoestudio/Curso		10	16-ene	28-abr																	

2.5 Equipo de Trabajo

Rol	*Responsabilidad*	*Nombre (opcional)*
Subdirector de Comunicaciones	Responsable de las telecomunicaciones del centro a nivel administrativo	
Subdirector de Sistemas	Responsable de los sistemas del centro a nivel administrativo	
Project Manager	Encargado de proyectos internos	
Administrador de Sistemas	Responsable de los sistemas de red y radio del centro a nivel operacional	
Técnico Especializado	Responsable de los sistemas de red y radio del centro a nivel de help desk	
Becario	Alumno en el proyecto PAP en radios	
Becario	Alumno en el proyecto PAP en sistemas	
Becario	Alumno en el proyecto PAP en sistemas	

2.6 Plan de Comunicaciones

Emisor	*Mensaje*	*Receptor*	*Medio*	*Frecuencia*

Responsable PAP	Información, Entregable	Grupo	Videoconferencia	D
Subdirector Telecom	Seguimiento de descubrimientos y targets	Grupo	Email	S
Subdirector Sistemas	Seguimiento de descubrimientos y targets	Grupo	Email	S
Project Manager	Seguimiento de objetivo a infraestructura	Estudiantes	Whatsapp	D
Técnico Especializado	Apoyo técnico	Estudiantes	Whatsapp	D
Estudiantes PAP	Seguimiento de descubirmientos	Estudiantes	Whatsapp	D

2.7 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.*
Subdirector Telecom	Targets para evaluar	Administrador de Sistemas	Debe de estar en el scope, entregado en tiempo y forma	Project Manager
Administrador de Sistemas	Preparado de infraestructura para evaluación	Project Manager	Servicios preparados para evaluación	Projet Manaher
Project mánager	Listado de targets	Alumnos PAP	Entregado con el scope adecuado	Administrador de Sistemas
Alumnos PAP	Avances de descubrimientos de vulnerabilidades, documentación, valoración	Ingenieros, Administrador de Sistemas, Técnico	Descubrimientos altamente detallados y evaluados conforme al criterios internos	Carpeta compartida de forma segura

2.8 Seguimiento y Control

Este proyecto está en progreso y se realizan dos visitas al centro cada semana para llevar a cabo las vulneraciones, documentaciones y análisis necesarios. Se establecen objetivos a evaluar cada semana, lo que permite realizar evaluaciones adecuadas y elaborar la documentación necesaria. Cada visita es una oportunidad para tomar nota de los avances y establecer planes de acción para la siguiente semana, garantizando así el cumplimiento total de los objetivos del proyecto.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

- Investigación sistema radiofrecuencia
- Reporte de vulnerabilidades
- Plan de mitigación de riesgos
- Documentación de herramientas

3.2 Estimación del Impacto

Con la colaboración de todos los involucrados en este PAP, se realizó de forma efectiva una evaluación a la ciberseguridad a la infraestructura de seguridad pública del estado de Jalisco. Este proyecto ayudará a miles de personas, desde el ámbito de seguridad informática, a que las telecomunicaciones utilizadas por los diferentes miembros de seguridad pública, entre bomberos, policía, fiscalía, etc. Estén salvaguardadas y protegidas contra ataques y malhechores.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

Para este proyecto PAP, desarrolle diversas competencias técnicas como lo son la detección e identificación de vulnerabilidades, el análisis de vulnerabilidades, la elaboración del plan de mitigación de riesgos, la instalación y uso de herramientas de monitoreo y detección de amenazas y el desarrollo de un reporte de vulnerabilidades y documentación. A su vez desarrolle competencias suaves como la autodisciplina, liderazgo, el trabajo en equipo y la facilidad de comunicación.

De forma social, pude involucrarme con una instancia gubernamental de seguridad pública, vi la problemática de como la seguridad informática es importante en todos y cada uno de los aspectos de nuestras vidas, al estar conectados y facilitarnos las tareas diarias con la tecnología, es de suma importancia estar protegida, más aún cuando se trata de un organismo en pro y ayuda de la ciudadanía. En este PAP pude aplicar un amplio catálogo de materias de mi carrera y conocimiento, desde los aprendizajes más técnicos hasta los más sociales, en especial la administración de proyectos, materias como la criminalística y materias propias de la ingeniería como vulnerabilidades y servicios de internet.

Me siento un poco más preparado para preparar un proyecto y completamente preparado para ser parte de él, seguir adelante con si seguimiento y colaborar con los compañeros para llegar al objetivo en común.

4.2 Aprendizajes Sociales

Pude innovar en el área de seguridad pública, evaluando, analizando, documentando e implementando diversas medidas para las vulnerabilidades y como mitigarlas. Este proyecto tiene la bondad de poder beneficiar a todos los sectores de la sociedad a nivel estatal ya que este organismo sobrelleva y coordina las diferentes dependencias de seguridad pública a nivel Jalisco. Cambio bastante mis supuestos sobre el gobierno y sus instituciones gubernamentales, aprendí sobre los diversos procesos y duras decisiones que deben tomar para llevar a cabo este tipo de iniciativas, además de involucrarme más con la ciudadanía desde la perspectiva de como protegerla y ayudarla. Pude aprender a ser mejor ingeniero en mi rama y aprendí a ser mejor líder para la toma de decisiones y mejor ciudadano para saber exactamente que hacer ante situaciones de emergencia.

4.3 Aprendizajes Éticos

Éticamente, mi trabajo involucra mucha información confidencial, si bien es bastante emocionante conocer los sistemas gubernamentales, ver su funcionalidad y extensión, como profesionales, debimos mantener todo este conocimiento desde el inicio del proyecto en adelante en total confidencialidad. Descubrir métodos para infiltrarme en los sistemas, elaborar reportes y mitigaciones, todo en pro de la ciudadanía. El trabajo involucra el tener la oportunidad de dejar un backdoor, un hueco especial para ti para tu futuro uso y ganancias personales. En esta línea laboral, la ética es absolutamente la base para lograr los objetivos. Después de esta experiencia, gusto seguir con proyectos de evaluaciones de seguridad, para trabajar siempre en pro de los clientes y llegar a tener un impacto cada vez mayor, aprendí a manejar esta clase de proyectos y como voy a ejercer mi profesión.

4.4 Aprendizajes Personales

Este PAP ha sido una experiencia única, pude trabajar en pro de la sociedad , me dio una nueva visión de lo que puede ser un trabajo, no necesariamente trabajar para ganar más dinero si no trabajar para beneficiar servicios que incluso yo pudiera necesitar. El estar trabajando y brindando servicios para el gobierno me ayudó a enseñado a ver cómo funciona el sistema de emergencias en Jalisco, entender la ayuda que brinda a la sociedad y comprender un poco los problemas que tienen estas instituciones.

4.5 Tareas Aprendidas

En este proyecto, pude notar que el trabajo en equipo fue la piedra angular de todo. Me ayudó a manejar mejor mis tiempos y a mejorar mi comunicación tanto técnica como no técnica. A su vez el hecho de que el Project mánager tuviera ordenado todo el trabajo para llegar por los objetivos de la semana y entregarlos fue bastante útil, veo la importancia de esa posición y aprendí a llevar un orden en mi propio trabajo. Por otra parte, el fijar rangos de presupuesto y explicar mejor los alcances son aprendizajes que llevé con esta experiencia, para dar una mejor comunicación entre cliente y proveedor.

5. Conclusiones

En conclusión, el proyecto PAP en IT Legal Services fue una experiencia muy valiosa que me permitió adquirir conocimientos y habilidades útiles para mi carrera profesional. Durante el proyecto, aprendí mucho sobre el trabajo en equipo, la importancia de la comunicación efectiva y la ética en el ámbito laboral.

Al principio, tuvimos algunos problemas para organizarnos y conocernos entre los colaboradores del proyecto, pero gracias a nuestra perseverancia y trabajo en equipo, logramos superar estos obstáculos y alcanzar nuestros objetivos. El proyecto requería un esfuerzo conjunto y personal. Además, durante el proyecto, enfrentamos varios desafíos técnicos que nos permitieron poner en práctica nuestras habilidades y conocimientos. A pesar de estos obstáculos, logramos resolverlos de manera efectiva gracias a la colaboración y el trabajo en equipo. Estoy agradecido por haber tenido la oportunidad de trabajar en un proyecto enriquecedor que me permitió crecer tanto personal como profesionalmente.

En resumen, el proyecto PAP en IT Legal Services fue una experiencia de aprendizaje muy valiosa que me permitió adquirir nuevos conocimientos y habilidades, y me enseñó la importancia del trabajo en equipo, la comunicación efectiva y la ética en el ámbito laboral. Estoy seguro de que los conocimientos adquiridos me serán de gran utilidad en mi carrera profesional futura.