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

PAP4N01A PROGRAMA DE LA INDUSTRIA DE ALTA TECNOLOGIA I

IT LEGAL SERVICES

PRESENTA

Alumno: ISI, Maya Alondra Aguirre Sayavedra

Profesor PAP: Juan Manuel Islas Espinoza, PMP®

Tlaquepaque, Jalisco, Mayo 2024

ÍNDICE

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 se enfoca en determinar el funcionamiento de un dispositivo proporcionado por una institución pública de seguridad del estado de Jalisco, así como advertir si este atenta contra la seguridad y/o privacidad de los ciudadanos. Por lo que el impacto de este proyecto recae en la población del estado y a la toma de decisiones de la institución para desarrollar alternativas relativas a la seguridad pública, con el fin de respetar la privacidad de los ciudadanos de Jalisco.

Este proyecto será coordinado por personal de la empresa IT Legal Services, la cual tiene como director general al Licenciado Carlos Durón, quien también es profesor de la universidad dentro del Departamento de Electrónica y Sistemas Informáticos (DESI). IT Legal Services es una firma legal que ofrece servicios relacionados a delitos cibernéticos, así como forense digital y recuperación de sistemas. Dentro de esta empresa, desarrollaré el rol de becaria, donde se me asignarán tareas para lograr el objetivo del proyecto y conocer los procesos internos de esta.

1. Introducción

1.1 Antecedentes

IT Legal Services es una firma especializada en temas de derecho informático y ciberdelitos, por lo que ofrece asesorías legales a casos relacionados con tecnología, donde en base a la evidencia encontrada se orienta a la persona para determinar qué, cómo, dónde y por qué sucedió el evento.

Aunque es una firma legal, no se limita a atención de la justicia, sino que también ofrece servicios de recuperación de incidentes, por lo que su campo de atención se extiende a organizaciones públicas y privadas afectadas por ransomware que no tienen un plan de contingencia o un plan poco efectivo, incluyendo pruebas de penetración a los sistemas como medio de prevención.

Es por ello que su misión es atender las necesidades tecnológicas de los afectados derivadas de un ataque cibernético desde el punto de vista ingenieril, penal y forense.

1.2 Justificación

Las ciencias forenses actualmente tienen un impacto significativo en la sociedad desde diversos ámbitos, como lo es el penal, la prevención y la cultura. Y ahora que estamos en la era digital, es de vital importancia concientizar a todas las personas, desde trabajadores de empresas hasta adultos mayores con acceso a una conexión a internet, ya que cualquier persona puede ser víctima de un delito donde se involucre la tecnología, como puede ser robo de identidad, estafas, filtración de datos personales, cifrado de información, entre otros. Por ello, se requiere brindar una asesoría clara y precisa acerca del delito en cuestión, donde la tecnología se utilizó como medio u objetivo (en el caso de cifrado de información o filtración), esto con el fin de brindar diversas soluciones a la víctima, y a su vez, facilitar herramientas para evitar futuras incidencias.

Para adquirir estas habilidades, si bien ITESO me ha brindado las bases suficientes para desarrollar las capacidades profesionales que se requieren en este campo, es necesario cumplir con un total de 15 – 20 horas semanales para poner en práctica mis conocimientos, a la vez que aprendo nuevas. IT Legal Services me facilitará las herramientas y guía necesaria para cumplir mis objetivos personales de crecimiento y los objetivos del proyecto.

En lo personal encuentro muy atractiva el área forense, en todas sus ciencias e ingenierías, esto porque creo que logra tocar varios ámbitos para explicar un suceso, desde la humanidad (como el comportamiento) hasta la física (gravedad, velocidad,

etc). Por esto decidí incorporarme a esta empresa, pues puedo especializarme, y a la vez conocer diversos puntos de vista de una situación.

1.3 Objetivos

IT Legal Services cree que actualmente la ciberseguridad es un área que debe ser desarrollada más rápido que la evolución tecnológica, ya que nos estamos enfrentando a diversas problemáticas éticas y legales, donde la Inteligencia Artificial es usada para fines delictivos o explotada para evadir sistemas de seguridad o filtrar información. Incluso ya no serán sólo problemas con computadoras o servidores, sino que se podrán cometer delitos como homicidio, esto por el avance de bio-hacking, el cual involucra colocar dispositivos inteligentes en alguna parte del cuerpo, como puede ser en los ojos, manos, brazos, corazón, etc. Por esta razón, IT Legal Services busca capacitar y estar a la vanguardia en temas tecnológicos para pensar en las consecuencias de las nuevas tecnologías, difundir sus contras, a la vez que se buscan soluciones ante estas problemáticas éticas y técnicas.

Mi objetivo dentro de la empresa es adquirir nuevos puntos de vista acerca de la tecnología para formar mi propia opinión y tener un panorama más amplio sobre los pros y contras de la evolución tecnológicas.

1.4 Contexto

El área en la que estaré trabajando es Evaluación de Seguridad con el rol de becario, donde estaré investigando y evaluando dispositivos, esto con el fin de conocer su funcionamiento y determinar su viabilidad para futura implementación por parte de una institución de seguridad pública.

1.5 Inventario de Competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	**Manejo de Office**	2	2	0	2	B
1.1	Fórmulas de Hojas de cálculo	1	2	0	2	B
1.2	Formatear editores de texto	1	2	0	2	B
2	**Comunicación oral y escrita**	3	3	0	3	M
2.1	Buena gramática y ortografía	3	3	0	3	A
2.2	Uso de lenguaje técnico y no técnico	3	2	1	3	A
3	**Búsqueda en navegador**	2	2	0	3	A
3.1	Uso de dorks para filtrar información	3	2	1	3	A
3.2	Uso de diversos motores de búsqueda	2	2	0	2	B
4	**Uso de software para análisis de tráfico**	3	2	1	3	A
4.1	Interpretar capturas de archivos pcap	3	2	1	3	A
4.2	Uso de líneas de comando en Linux	2	2	0	3	A
4.3	Uso de líneas de comando en Windows	2	2	0	3	A
5	**Interpretación de esquemas electrónicos**	1	1	0	1	B
5.1	Leer data sheets de dispositivos electrónicos	1	1	0	1	B
6	**Documentación de procesos**	3	3	0	3	A
6.1	Uso de una metodología técnica	2	2	0	3	M
6.2	Presentación de resultados	2	2	0	3	M
6.3	Consulta de información en fuentes confiables	3	3	0	3	A
6.4	Citar fuentes en formato APA y/o IEEE	2	2	0	2	M

1.6 Plan Educativo

Plan de Actividades

No.	Actividad Educativa	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	**Manejo de hojas de cálculo**																		
1.1	Tomar cursos nivel intermedio para uso de hojas de cálculo	15/01/2024	20/01/2024																
1.2	Crear ejercicios en diferentes contextos	15/01/2024	27/01/2024																
1.3	Aplicar conocimiento en los documentos necesarios	29/01/2024	16/05/2024																
2	**Uso de software para análisis de tráfico**																		
2.1	Tomar cursos nivel intermedio de Wireshark	05/02/2024	16/02/2024																
2.2	Realizar ejercicios para interpretar las capturas	05/02/2024	16/05/2024																
3	**Uso de líneas de comando**																		
3.1	Buscar documentación de líneas de comando en SO Windows básicos-intermedio	19/02/2024	16/05/2024																
3.2	Buscar documentación de líneas de comando en SO Linux básicos-intermedio	19/02/2024	16/05/2024																
3.3	Crear scripts de práctica para cada SO	19/02/2024	16/05/2024																
4	**Documentación de procesos**																		
4.1	Aprender metodología que la empresa tiene implementada	15/01/2024	09/02/2024																

1.7 Entregables

A lo largo del proyecto, se tendrán dos entregables:

1. Reporte de actividades mensual de manera individual.
2. Reporte final de evaluación, el cual incluye el desarrollo del proyecto con evidencia que sustente los pasos y conclusiones.

1.8 Involucrados

IT Legal Services al brindar servicios a instituciones públicas y privadas, los resultados de este proyecto benefician: a la Dirección de Tecnología y Dirección General del organismo de seguridad pública del estado de Jalisco.

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

Al ser un proyecto que tiene como objetivo conocer el funcionamiento de un dispositivo con el fin de determinar las consecuencias de privacidad o si atenta contra la ciberseguridad de los dispositivos inteligentes, sólo se llevarán a cabo las etapas de Inicio, Planificación, Seguimiento y Cierre.

En la etapa de inicio se determinan los objetivos y propósitos clave para desarrollar el proyecto, en la planificación, se establecen las tareas principales con sus subtareas a realizar para cumplir los objetivos descritos anteriormente. Una vez descritas las tareas, con su fecha inicio y término, así como los encargados, se procede a la etapa de ejecución, donde se desarrollan las tareas establecidas por el equipo correspondiente, respetando las fechas límite. En la etapa de seguimiento, se harán juntas presenciales y/o virtuales para conocer los avances de cada equipo, así como las necesidades o problemas que van surgiendo. Al finalizar el proyecto, se entregará un informe final sobre los resultados, así como las conclusiones generales y personales técnicas de lo que se encontró del funcionamiento del dispositivo.

2.2 Sustento Teórico y Metodológico

Al ser un proyecto dedicado a la investigación y usos de procesos forenses, la metodología a utilizar será el Análisis forense, la cual consta de las siguientes fases:

1. Planteamiento del problema: se evalúa el problema y se determina el alcance del mismo y la posible solución.
2. Identificación: se conocen los procesos internos de la empresa, así como la capacidad profesional del personal designado para controlar la situación y/o el equipo técnico involucrado. Con la información obtenida, se crea el plan de acción para adquirir la evidencia, cuidando la cadena y su preservación.
3. Adquisición: se eligen los métodos apropiados para obtener copia del hardware de almacenamiento y/o capturas de tráfico de red, esto teniendo una lista de prioridad para su atención.
4. Preservación: Se hacen 1-2 copias de la información obtenida previamente, con el fina de conservar la cadena de custodia y evitar corrupción de archivos. Estas copias son las que se utilizarán para hacer el análisis.
5. Análisis: se establecen las herramientas y técnicas a utilizar para estudiar el material obtenido y comenzar a hacer deducciones de lo ocurrido,

documentando los pasos elaborados. Esto con el objetivo de crear una línea temporal y determinar qué, cómo, quién, con qué se llevaron a cabo las acciones y su impacto.

6. Presentación: Se recopila la información de las fases anteriores y se prepara la documentación para redactar un informe final de los eventos, el cual contiene el asunto, resumen, evidencias y detalles, conclusiones y documentación de apoyo.
7. Fin: se devuelve la evidencia y se destruyen las copias almacenadas y/o documentación impresa de carácter confidencial, con el objetivo de no violar la privacidad de la empresa o divulgación de información sensible de clientes o personal de la empresa.

2.3 Descripción del Proyecto

El proyecto tiene como objetivo encontrar el funcionamiento de un dispositivo y concluir sobre el impacto que pueda tener sobre la ciberseguridad y privacidad de las personas, por lo que el ciclo de vida será tipo Evolutivo, ya que los requerimientos pueden crecer o decrecer conforme se tenga más información del dispositivo a estudiar. De manera general, las tareas que se realizarán en cada fase son:

1. Planificación: creamos un plan inicial y se dividen las tareas principales por equipo según las habilidades de cada uno.
2. Análisis de riesgos: establecemos los riesgos que puedan surgir, ya se de manera interna o externa, al igual que un plan de contingencia para aminorar el impacto del riesgo, en dado caso que suceda.
3. Ingeniería: cada equipo establece su metodología, fechas de inicio y término de cada sub-tarea, así como el representante del equipo.
4. Evaluación: Se harán reuniones presenciales y/o virtuales para compartir los avances y establecer si se requiere ampliar el alcance de la investigación y/o actualizar el análisis de riesgo, o cambiar la metodología o herramientas.

Estas fases principales se llevarán a cabo iterativamente hasta encontrar todos los riesgos que engloben en el objetivo principal del proyecto.

2.4 Plan de Trabajo

Plan de Actividades

No.	Actividad Educativa	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Estado
1	**Inducción**																			
1.1	Tomar cursos de inducción	15/01/2024	19/01/2024																	F
1.2	Realizar actividades con supervisor asignado para conocer los procesos	15/01/2024	26/01/2024																	F
1.3	Inducción al proyecto	15/01/2024	19/01/2024																	F
2	**Desarrollo de proyecto**																			
2.1	Establecer riesgos y plan de contingencia	29/01/2024	15/05/2024																	P
2.2	Identificar componentes y especificaciones	29/01/2024	15/05/2024																	P
2.3	Identificar funcionamiento de componentes	29/01/2024	15/05/2024																	P
2.3.1	Leer capturas de red	29/01/2024	15/05/2024																	P
2.3.2	Analizar imagen de disco	29/01/2024	15/05/2024																	P
																				P
3	**Documentación**																			
3.1	Realizar reporte de actividades	15/01/2024	15/05/2024																	P
3.2	Realizar reporte de avances	15/01/2024	15/05/2024																	P
3.3	Reporte documentado del dispositivo investigado	29/01/2024	15/05/2024																	P
4	**Conclusión**																			
4.1	Entregar reporte final	15/05/2024	16/05/2024																	P
4.2	Presentación de proyecto	15/05/2024	16/05/2024																	P

2.5 Equipo de Trabajo

Rol	*Responsabilidad*	*Nombre (opcional)*
Coordinador de Proyecto	*Dar seguimiento a los avances del proyecto, comunicar actualizaciones del proyecto, facilitar herramientas y documentación requerida*	
Coordinador de equipo	*Dar seguimiento a los avances de cada integrante, resolver dudas, presentar avances mensuales del proyecto, comunicar las actualizaciones del proyecto a los miembros del equipo*	
Líder técnico	*Valida los planes de trabajo y realiza observaciones en base a los avances presentados, asistencia de soporte en caso de problemas con un equipo o software, da accesos a las herramientas*	
Becario	*Sigue el plan de trabajo, recibe capacitaciones para desarrollar las tareas, reporta sus actividades de manera mensual*	

2.6 Plan de Comunicaciones

Emisor	*Mensaje*	*Receptor*	*Medio*	*Frecuencia*
Coordinador de equipo	*Presentación de avances*	*Coordinador de proyecto*	*Video conferencia*	*M*
Becario	*Presentación de avances, dudas, aclaraciones*	*Coordinador de equipo*	*Video conferencia*	*2S*
Coordinador de equipo	*Reporte de avances*	*Coordinador de proyecto*	*Correo*	*M*
Becario	*Reporte de actividades*	*Coordinador de equipo, Coordinador de proyecto*	*Correo*	*M*

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.*
Becario	*Reporte de actividades*	*Coordinador de proyecto*	*Fecha de elaboración, rango de días del mes a entregar, nombramiento y responsabilidades, firma en tinta azul del que reporta, uso de membrete empresarial*	*Expediente de RRHH*
Coordinador de equipo	*Reporte de avances*	*Coordinador de proyecto*	*Fecha de elaboración, resumen ejecutivo, justificación, listado de tareas realizadas, conclusiones, uso de membrete empresarial*	*Documentación de proyecto*
Coordinador de equipo	*Reporte final*	*Coordinador de proyecto*	*Fecha de elaboración, resumen ejecutivo, justificación, tareas principales realizadas documentadas, conclusiones, recomendaciones, uso de membrete empresarial*	*Documentación de proyecto*

2.8 Seguimiento y Control

El líder del equipo, de manera quincenal, recibe los avances por parte de los becarios de las actividades realizadas en el transcurso de esos días, al igual que si surgen problemas para el desarrollo o dudas de implementación o sobre algunos procesos. Donde las dudas y problemas se pueden resolver en la misma sesión, si es posible, si no, se tiene el rango de una semana para solución y se da seguimiento semanal o quincenal, dependiendo la gravedad o la importancia de la situación.

En cuanto al reporte de que envía y presenta el coordinador del equipo, es revisado por el coordinador de proyecto de manera mensual para lograr observar cambios significativos y saber si se tiene que repetir un proceso o modificar los alcances o adquirir más herramientas, en dado caso que exista una situación que no pueda esperar a verse dentro de cuatro semanas, se hace de conocimiento a la brevedad al coordinador del proyecto para iniciar un plan de contingencia o acciones correctivas, según la severidad del impacto.

Los entregables que los becarios envían de manera mensual, es revisado por el coordinador de proyecto de la empresa y los resultados de los avances se exponen en el entregable final de la materia PAP ofrecida por la universidad ITESO, donde el profesor evalúa la calidad de la gramática y el uso de la plantilla del reporte, con el fin de dar retroalimentación de manera organizada e individual a cada compañero de la clase y obtener los puntos necesarios para acreditar el PAP.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

1. Reporte mensual de actividades.
2. Reporte final de proyecto.

3.2 Estimación del Impacto

El reporte final contiene las conclusiones sobre el impacto en aspectos legales o de privacidad del dispositivo, por lo que la institución que solicitó esta investigación tomará en cuenta estos resultados para tomar la mejor decisión y/o crear un plan de riesgos para mitigarlos o disminuir su impacto.

Es por ello que el trabajo realizado en este proyecto es importante, ya que conlleva a una toma de decisiones a nivel estatal que puede llevar consecuencias legales si no se hace un análisis profundo de la situación.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

- Uso de herramientas para análisis forense.
- Metodología de análisis forense.
- Búsqueda avanzada en buscadores web.
- Uso de comandos de línea en Windows y Linux.
- Documentar y presentar reportes técnicos.
- Análisis de riesgos.
- Crear planes de contingencia.

4.2 Aprendizajes Sociales

El objetivo del proyecto era conocer las implicaciones de implementar un dispositivo según su funcionamiento, por lo que la aportación social que surgió fue hacer consciencia del uso de la tecnología en el ámbito de la seguridad pública y cuestionar hasta dónde podemos obtener o no información sensible de la población.

4.3 Aprendizajes Éticos

El ámbito de la seguridad pública y la ciberseguridad puede convertirse en actividades grises donde podemos llegar a lo ilegal con un solo paso, ya que podemos pensar que hacer lo correcto sin importar el cómo es mejor, pero debemos ser conscientes que esas acciones siempre tendrán consecuencias a corto o largo plazo, incluso perjudicar el profesionalismo y la ética de la institución a la que se representa. Por ello, es importante cultivar valores y ética que la institución debe reflejar en sus procesos, misión y visión, con el fin de establecer los límites necesarios y motivar al personal a ponerlos en práctica.

4.4 Aprendizajes Personales

El desarrollo de este proyecto me ha motivado a buscar la manera de emplear la tecnología de forma responsable, donde pueda ayudar de mejor manera a los usuarios finales, así como prevenir a la población que tiene menos contacto con ella a ser víctimas de delitos cibernéticos. También me ha ayudado a hacer una introspección sobre el desarrollo imparable de la tecnología y cómo la privacidad y nuestros datos personales están dentro del mercado; esto con el objetivo de buscar alternativas para mantener mi información lo más privada posible.

4.5 Tareas Aprendidas

En el PAP, como en cualquier proyecto, se presentaron problemas, pero que con una buena coordinación y comunicación se lograron resolver, lo cual fomenta el trabajo en equipo y la resolución de problemas. Es importante de igual manera, conocer la cadena de mando y los procesos internos de la empresa para tener mayor precisión en las decisiones a tomar, según la gravedad y alcance de la situación.

En lo personal, me ayudó mucho el apoyo de mis coordinadores, al igual que su paciencia para entender y aprender los procesos a seguir según la naturalidad de la situación o problema que surgía, al igual que la apertura de realizar mis tareas a mi ritmo y mis propios procesos.

5. Conclusiones

Mi proyecto PAP fue interesante y representó un reto personal y profesional, pues a pesar de contar con ciertas habilidades requeridas para realizar las tareas asignadas en mi puesto, fue necesario pulirlas y desarrollarlas aún más para alcanzar los objetivos a los estándares de la empresa y personales. Me fue agradable convivir con profesionales de diversas áreas, pues al ser un despacho jurídico, aprendes procesos de licenciaturas humanistas, y así enriqueces tus conocimientos técnicos, con el fin de especializar las prácticas y adquirir habilidades diferenciadoras al momento de una entrevista laboral.