

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: IS, JUAN FELIPE GUDIÑO RAMOS

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

Tlaquepaque, Jalisco, Julio 2024

ÍNDICE

Contenido

REPORTE PAP	3
<i>Presentación Institucional de los Proyectos de Aplicación Profesional.....</i>	<i>3</i>
Resumen	4
1. Introducción	5
1.1 Antecedentes.....	5
1.2 Justificación.....	5
1.3 Objetivos	5
1.4 Contexto.....	6
1.5 Inventario de Competencias.....	6
1.6 Plan Educativo	6
1.7 Entregables	6
1.8 Involucrados	6
2. Desarrollo del Proyecto PAP	7
2.1 Administración del Proyecto	7
2.2 Sustento Teórico y Metodológico.....	7
2.3 Descripción del Proyecto.....	8
2.4 Tipo de Proyecto	9
2.5 Plan de Trabajo.....	9
2.6 Equipo de Trabajo	10
2.7 Plan de Comunicaciones	10
2.8 Plan de Calidad.....	11
2.9 Seguimiento y Control	11
2.10 Cierre del Proyecto	12
3. Resultados del Trabajo Profesional.....	13
3.1 Productos Obtenidos	13
3.2 Estimación del Impacto	13
4. Reflexiones del alumno	14
4.1 Aprendizajes Profesionales	14
4.2 Aprendizajes Sociales	14
4.3 Aprendizajes Éticos.....	14
4.4 Aprendizajes Personales.....	14
4.5 Tareas Aprendidas.....	14

4.6 Desarrollo Profesional	15
5. Conclusiones	15
6. Bibliografía y Anexos (<i>en caso de ser necesarios</i>).....	15

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

Durante el desarrollo del proyecto PAP de Primavera 2024, trabajamos en conjunto con la empresa IT Legal Services para la ejecución de un proyecto de análisis de filtración de documentos, de análisis de metadatos de los documentos filtrados, de implantación de un documento de análisis de la red interna, para analizar el comportamiento de los usuarios internos.

Durante el desarrollo del reporte se especifica la justificación, Objetivo y metodología utilizada para la realización del proyecto, detallando las habilidades a desarrollar para el cumplimiento de los entregables solicitados y su plan de trabajo de capacitación.

Durante el proceso de aproximadamente 2 meses se llevo acabo el proyecto, definiendo a grandes rasgos las siguientes etapas:

- 1. Planeación y capacitación**
- 2. Investigación y análisis**
- 3. Definición de conclusiones**
- 4. Preparación de reportes de hallazgos.**

Las cuales nos ayudaron a desarrollar distintas habilidades, tanto profesionales, sociales y personales, dando una base a nuestra formación como profesionales con y para los demás, preparándonos y dándonos una introducción al mundo laboral profesional.

1. Introducción

1.1 Antecedentes

IT Legal Services es una firma especializada en derecho informático y cibercriminalidad. Aborda cuestiones tecno-legales desde una perspectiva legal, técnica y forense.

La empresa se centra principalmente en ofrecer servicios a pymes y clientes particulares, con un enfoque de mercado local, aunque ocasionalmente atiende clientes en Norteamérica y América Latina.

IT Legal Services se esfuerza por proporcionar un servicio de alta calidad a precios competitivos, destacando la honestidad y el compromiso moral. En algunas ocasiones, también toma casos pro bono como parte de su labor social.

1.2 Justificación

Actualmente, las ciencias forenses tienen un impacto considerable en la sociedad, abarcando ámbitos como el penal, la prevención y la cultura. Con la transición a la era digital, es esencial concienciar a todos, desde empleados corporativos hasta adultos mayores con acceso a internet, ya que cualquiera puede ser víctima de delitos tecnológicos como el robo de identidad, estafas, filtración de datos personales o cifrado de información.

Por ello, es crucial proporcionar asesoría clara y precisa sobre estos delitos, especialmente cuando la tecnología se utiliza como medio u objetivo, como en los casos de cifrado de información o filtración de datos. El objetivo es ofrecer soluciones efectivas a las víctimas y, al mismo tiempo, suministrar herramientas para prevenir futuros incidentes.

He tenido experiencia previa en el área de forense informática a través de diversos cursos y certificaciones, lo que me hace encontrar muy interesante a esta empresa y sus actividades. Considero que puede ser muy valiosa para mi desarrollo profesional. Con mis conocimientos adquiridos dentro y fuera de la universidad y en IT Legal, podremos realizar investigaciones y peritajes adecuados para apoyar a diversas organizaciones.

1.3 Objetivos

Mi objetivo es, en conjunto con la empresa, desarrollar y mejorar las metodologías forenses, realizando distintos análisis en conjunto con diversas organizaciones, para ejercitar, identificar y mejorar los métodos de análisis forenses de la organización.

Espero poder fortaleciendo y desarrollando mis competencias de:

- Análisis forense
- Comunicación interdepartamental
- Gestión de proyectos

1.4 Contexto

El área en la que estaré trabajando es Evaluación de Seguridad con el rol de becario, donde estaré investigando y filtraciones de información sensible hacia la red, y analizando su origen, adicional realizaremos pruebas de ingeniería social hacia una organización en específico para evaluar su conocimiento en temas básicos de ciberseguridad.

1.5 Inventario de Competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	Ejecución de herramientas forenses	4	2	2	2	A
1.1	Uso de estenografía	2	1	1	2	A
1.2	Uso de foca	2	1	1	2	M
2	Generación de reportes de análisis	2	2	0	2	A
2.1	Desarrollo de reportes técnicos	2	2	0	2	A
3	Manejo de paquetería de ofimática	2	2	0	2	A
3.1	Generación de presentaciones ejecutivas en PPW	2	2	0	2	M
3.2	Generación de reportes detallados en Word	2	3	1	2	A

1.6 Plan Educativo

No.	Actividad Educativa	Tipo Actividad	Total Hrs	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	Obj
1	Capacitación sobre herramientas forenses													
1.1	Capacitación sobre uso de Estenografía	Curso	15	03/06/2024	14/06/2024									
1.2	Capacitación sobre uso de foca	Curso	15	17/06/2024	28/06/2024									
2	Capacitación sobre desarrollo de procesos													
2.1	Capacitación de mejora de desarrollo de reportes técnicos	Estudio	10	01/07/2024	12/07/2024									

1.7 Entregables

A lo largo del proyecto se entregará:

- Reporte de filtrado de información sensible
- Reporte de ingeniería social

1.8 Involucrados

- IT Legal Services
- 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

- **Inicio:** Establecer los objetivos y metas a lograr en el proyecto, alcance y limitantes.
- **Planificación:** Definición de tareas e hitos para cumplir los objetivos. Encargados y responsables de actividades.
- **Ejecución:** Ejecución de las tareas descritas en la etapa de planificación.
- **Seguimiento y control:** Ejecución de juntas de seguimiento y resolución de problemas y dudas durante el proyecto.
- **Cierre:** Entrega de reportes y entregables definidos.

2.2 Sustento Teórico y Metodológico

1. Preparación

- **Definir el Alcance del Análisis:** Establecer los límites del análisis, incluyendo los sistemas, datos y redes involucradas.
- **Reunir Equipo y Herramientas:** Asegurarse de contar con un equipo multidisciplinario y las herramientas necesarias (software de análisis forense, herramientas de monitoreo de red, etc.).
- **Establecer Protocolos de Comunicación:** Definir cómo se comunicará el equipo durante el análisis y cómo se reportarán los hallazgos.

2. Identificación y Recolección de Datos

- **Detección de Incidentes:** Utilizar sistemas de detección de intrusiones (IDS) y sistemas de información y gestión de eventos de seguridad (SIEM) para identificar incidentes.
- **Recolección de Evidencia:** Recopilar registros de logs, archivos de sistema, correos electrónicos y cualquier otro dato relevante que pueda ser evidencia de la filtración.
- **Asegurar la Cadena de Custodia:** Documentar cada paso en la recolección y manejo de evidencia para mantener la integridad de los datos.

3. Análisis

- **Examinación Inicial:** Revisar los datos recolectados para identificar patrones y anomalías que indiquen una filtración.
- **Análisis de la Fuente:** Identificar cómo y dónde ocurrió la filtración. Esto puede incluir análisis de malware, análisis de tráfico de red y revisión de permisos de acceso.
- **Determinación del Alcance:** Evaluar la magnitud de la filtración, incluyendo qué información fue comprometida y cuántos datos fueron afectados.

4. Mitigación

- **Contención del Incidente:** Implementar medidas inmediatas para detener la filtración y prevenir daños adicionales. Esto puede incluir el aislamiento de sistemas comprometidos.
- **Remediación:** Eliminar cualquier acceso no autorizado, corregir vulnerabilidades y restaurar sistemas a su estado seguro.

5. Informe y Documentación

- **Documentación del Análisis:** Crear un informe detallado que describa el incidente, el análisis realizado, los hallazgos y las acciones tomadas.
- **Recomendaciones:** Proporcionar recomendaciones para mejorar la seguridad y prevenir futuras filtraciones. Esto puede incluir cambios en políticas, mejoras en la infraestructura de seguridad y capacitación de empleados.

6. Seguimiento y Evaluación

- **Monitoreo Continuo:** Implementar monitoreo continuo para detectar posibles futuras filtraciones.
- **Evaluación Post-Incidente:** Revisar la respuesta al incidente para identificar áreas de mejora en la metodología y en las prácticas de seguridad.

7. Capacitación y Mejora Continua

- **Capacitación del Personal:** Asegurarse de que todo el personal esté al tanto de las mejores prácticas de ciberseguridad y del manejo de información sensible.
- **Actualización de Procedimientos:** Revisar y actualizar regularmente las políticas y procedimientos de seguridad para mantenerse al día con las nuevas amenazas y tecnologías.

2.3 Descripción del Proyecto

El objetivo del proyecto es realizar un análisis de filtrado de información sensible hacia la red, para identificar el alcance de la filtración y el origen de la misma, adicionalmente se realizarán ejercicios de ingeniería social dentro de la infraestructura del cliente, para evaluar la cultura organizacional respecto a la ciberseguridad.

De manera general se realizarán las siguientes fases:

- Identificación y recolección de datos:
- Análisis
- Informe y documentación
- Ejercicio de ingeniería social

2.4 Tipo de Proyecto

El tipo de proyecto se podría considerar en cascada, puesto que, de acuerdo a conforme se vayan liberando los entregables será la retroalimentación obtenida y el marco para el avance del proyecto.

2.5 Plan de Trabajo

No.	Competencia	Nivel Adquirido al Inicio	Nivel Objetivo al final PAP	Objetivo final PAP	Prior
1	Uso de estenografía	2	3	3	A
2	Uso de foca	2	3	3	M
3	Desarrollo de reportes técnicos	2	1	2	A
4	Generación de presentaciones ejecutivas en PPW	2	2	2	M
5	Generación de reportes detallados en Word	2	2	2	A

No.	Actividad Educativa	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8
1	Inducción										
1.1	familiarizarse con las herramientas	20/05/2024	31/05/2024								
1.2	Inducción al proyecto	27/05/2024	31/05/2024								
2	Desarrollo del proyecto										
2.1	Realizar recopliación de información	03/06/2024	28/06/2024								
2.2	Análisis y conclusiones de información filtrada	03/06/2024	28/06/2024								
2.3	Ejercicio de ingeniería social	03/06/2024	28/06/2024								
3	Documentación										
3.1	Realizar reportes de hallazgos	01/07/2024	05/07/2024								
4	Conclusión										
4.1	Entrega de reporte final	08/07/2024	12/07/2024								

2.6 Equipo de Trabajo

<i>Rol</i>	<i>Responsabilidad</i>	<i>Nombre (opcional)</i>
<i>Coordinador de Proyecto</i>	<i>Dar seguimiento a los avances del proyecto, comunicar actualizaciones del proyecto, facilitar herramientas y documentación requerida</i>	
<i>Coordinador de equipo</i>	<i>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</i>	
<i>Líder técnico</i>	<i>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</i>	
<i>Becario</i>	<i>Sigue el plan de trabajo, recibe capacitaciones para desarrollar las tareas, reporta sus actividades de manera mensual</i>	

2.7 Plan de Comunicaciones

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

2.8 Plan de Calidad

Emisor: <i>Quién Entrega</i>	Entregable: <i>Qué Entrega (SubEntregable)</i>	Receptor: <i>Quién recibe o Inspecciona</i>	Criterios: <i>Condiciones de Aceptación</i>	Siguiente paso. <i>Donde va Cuando se Autoriza.</i>
<i>Becario</i>	<i>Reporte de actividades</i>	<i>Coordinador de proyecto</i>	<i>Fecha de elaboración, rango de días del mes a entregar, nombramiento y responsabilidades, firma en tinta azul del que reporta, uso de membrete empresarial</i>	<i>Expediente de RRHH</i>
<i>Coordinador de equipo</i>	<i>Reporte de avances</i>	<i>Coordinador de proyecto</i>	<i>Fecha de elaboración, resumen ejecutivo, justificación, listado de tareas realizadas, conclusiones, uso de membrete empresarial</i>	<i>Documentación de proyecto</i>
<i>Coordinador de equipo</i>	<i>Reporte final</i>	<i>Coordinador de proyecto</i>	<i>Fecha de elaboración, resumen ejecutivo, justificación, tareas principales realizadas documentadas, conclusiones, recomendaciones, uso de membrete empresarial</i>	<i>Documentación de proyecto</i>

2.9 Seguimiento y Control

El líder del equipo recibe actualizaciones quincenales de las actividades realizadas por los becarios durante ese período. Además, se informa sobre posibles problemas de desarrollo o dudas de implementación y procesos. En caso de dudas o problemas, se busca resolverlos durante la misma sesión; de lo contrario, se dispone de una semana para encontrar soluciones, con seguimiento semanal o quincenal según la gravedad o importancia de la situación.

El coordinador del proyecto revisa mensualmente el informe de avances realizados por los becarios. Esto se hace con el fin de identificar cambios significativos y determinar si es necesario repetir un proceso, ajustar los alcances o adquirir más herramientas. Si surge una situación que no puede esperar hasta la revisión mensual, se comunica de inmediato al coordinador del proyecto para implementar un plan de contingencia o acciones correctivas, dependiendo de la gravedad del impacto.

Los entregables mensuales enviados por los becarios son evaluados por el coordinador del proyecto de la empresa. Los resultados de los avances se incluyen en el entregable final de la materia PAP de la Universidad ITESO. Donde el profesor evalúa el contenido del mismo, proporcionando retroalimentación a cada estudiante.

2.10 Cierre del Proyecto

En su momento si se tuvo una etapa de cierre de proyecto, de un proyecto que se podría considerar hermano, puesto que, de manera similar, ambos tienen un enfoque forense, aunque sean distintos en habilidades técnicas y objetivo final. En su momento se tuvo una retroalimentación satisfactoria y se hicieron notar los puntos a mejorar. Espero esta segunda entrega cumpla de igual manera con las expectativas y se pueda denotar mejora en las habilidades sugeridas al cierre del proyecto pasado.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

- Reporte de documentos filtrados
- Análisis de documentos filtrados
- Archivo de análisis de red
- Reporte de análisis de red interna.

3.2 Estimación del Impacto

La ejecución de este proyecto tiene un impacto a toda la población de Jalisco, pues, el filtrado de información del C5 es un tema muy sensible y que denota una falta de ética para algunos de los trabajadores del lugar, la identificación y aplicación de reglas de seguridad para evitar esta situación a futuro, favorecerá a la población Jalisciense en general, al tener un C5 más seguro, para el bienestar de la población.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

- Mejore mis técnicas de OSINT.
- Pulí y mejore mis técnicas de generación de reportes técnicos y ejecutivos
- Mejore mis técnicas de estenografía.

4.2 Aprendizajes Sociales

- Este proyecto a pesar de no tener una interacción directa con la sociedad, es de un alto impacto social al tratarse de asegurar una de las instalaciones de seguridad más importantes de Jalisco, teniendo un impacto claro en toda la sociedad Jalisciense.

4.3 Aprendizajes Éticos

- Este proyecto a pesar de no tener una interacción directa con la sociedad, es de un alto impacto social al tratarse de asegurar una de las instalaciones de seguridad más importantes de Jalisco, teniendo un impacto claro en toda la sociedad Jalisciense.

4.4 Aprendizajes Personales

- Durante el desarrollo del proyecto, además de los aprendizajes profesionales, me ayudó a aplicar y reforzar los aprendizajes que traía del pap anterior respecto a la organización, asegurando la entrega en tiempos, y apegándome al calendario de entregas.

4.5 Tareas Aprendidas

- Algo que nos sirvió como factor crítico de éxito durante la gestión del proyecto fue el apoyo y seguimiento de la gerencia de IT Legal Services para la atención de dudas respecto a los análisis realizados

4.6 Desarrollo Profesional

Durante el ejercicio de desarrollo profesional quedo plasmada de manera muy clara el camino que quiero tomar para mi vida profesional, este proyecto pap me ayudo a reforzar y entender algunas áreas un poco distintas a mi operación diaria, pero que también es necesario que aplique para mis futuros clientes.

Adicionalmente me ayudo a comprender un poco más de como funcionan otras organizaciones y los servicios que se pudieran ofrecer a las instituciones publicas.

Por ultimo me ayudo a reforzar mis habilidades tecnológicas para aplicarla con mis clientes, ofrecer nuevos servicios y poderme desenvolver de mejor manera.

5. Conclusiones

Durante la ejecución del proyecto PAP, a través de sus distintas etapas se vivieron varias experiencias, yendo desde la frustración hasta el orgullo de haber identificado algún hallazgo significativo y el cumplimiento del propósito del análisis.

Logre desarrollar diversas habilidades, pero las que mas destaco son la organización y la presentación adecuada de resultados, que nos fueron solicitados por la empresa, estando a la altura de la misma, cumpliendo los estándares de calidad requeridos, validando la veracidad de la información antes de generar una conclusión.

Quede muy satisfecho con la realización del PAP pues me ayudo a comprender una realidad y forma de trabajar de manera profesional distinta que con la que he estando trabajando durante muchos años, exigiéndome desarrollar competencias distintas a las que he llegado a desarrollar a lo largo de mi carrera universitaria.

6. Bibliografía y Anexos (*en caso de ser necesarios*)

Para la realización de este reporte PAP no fue necesario citar referencias externas.