

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

BISHOP FOX

PRESENTA

Alumno: ISI Sarah Lizeth MURIEL Ramirez

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

Tlaquepaque, Jalisco, diciembre de 2022.

ÍNDICE

Contenido

REPORTE PAP	2
Presentación Institucional de los Proyectos de Aplicación Profesional	2
Resumen	3
1. Introducción	4
1.1 Antecedentes	4
1.2 Justificación	4
1.3 Objetivos	4
1.4 Contexto	4
1.5 Entregables.....	5
1.6 Involucrados.....	5
2. Desarrollo del Proyecto PAP	6
2.1 Administración del Proyecto	6
2.2 Sustento Teórico y Metodológico	6
2.3 Descripción del Proyecto	6
2.4 Plan de Trabajo	7
2.5 Equipo de Trabajo	8
2.6 Plan de Comunicaciones.....	8
2.7 Plan de Calidad	8
2.8 Seguimiento y Control	8
2.9 Cierre del Proyecto.....	9
3. Resultados del Trabajo Profesional	10
3.1 Productos Obtenidos.....	10
3.2 Estimación del Impacto	10
4. Reflexiones del alumno	11
4.1 Aprendizajes Profesionales	11
4.2 Aprendizajes Sociales	11
4.3 Aprendizajes Éticos	12
4.4 Aprendizajes Personales	12
4.5 Tareas Aprendidas	12
4.6 Desarrollo Profesional	13
5. Conclusiones	14
6. Bibliografía y Anexos (solo en caso necesario)	Error! Bookmark not defined.

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 trabajo ha sido elaborado con el objetivo de exponer las características del Proyecto PAP, abarcando la información de la empresa huésped y detalles sobre el proyecto en el que se participa dentro de ella, así como los resultados obtenidos e impactos del proyecto tanto en el ámbito profesional como en el personal.

1. Introducción

1.1 Antecedentes

Bishop Fox es una de las empresas líder en el ámbito de la seguridad informática, proveyendo soluciones principalmente en las áreas de pruebas de penetración, administración de superficies de ataque, y evaluaciones de seguridad. La empresa brinda sus servicios a las principales empresas tecnológicas más importantes a nivel mundial, enfocándose en la seguridad ofensiva, asistiendo en el descubrimiento para la eliminación de vulnerabilidades antes de que puedan ser explotadas.

1.2 Justificación

Bishop Fox busca expandir la capacidad de operación de sus servicios, contando con un mayor número de personal que habilite el crecimiento de la compañía.

Mi razón principal para participar en este PAP es el poder desarrollar mis habilidades en el área específica de la seguridad informática en la que busco especializarme. A través de mi formación universitaria he adquirido conocimientos básicos para la interacción con la seguridad informática, con los cuales he podido desarrollar conocimientos y habilidades específicos para desarrollar el trabajo que realizo en mi puesto dentro de la compañía. Realizare veinte horas de trabajo dentro de la empresa a la semana, durante las cuales llevare a cabo las tareas asignadas para mi puesto dentro de la misma.

Planeo continuar en esta línea de negocio dentro de Bishop Fox posteriormente a mi graduación.

1.3 Objetivos

El entregable final más importante del proyecto serán notificaciones y reportes respecto al descubrimiento y validación de superficies de ataque pertenecientes al cliente.

Mis objetivos de aprendizaje son consolidar el conocimiento que he adquirido durante mi experiencia como intern con la compañía, alistándome para tomar una posición como analista al finalizar este periodo de aprendizaje.

1.4 Contexto

Dentro del proyecto en el que estaré participando se espera entregar al cliente el nivel de servicio estipulado respecto a la administración de su superficie de ataque durante la duración de su contrato, realizando el descubrimiento de la superficie de ataque de manera periódica, y su validación constante para habilitar el trabajo de

pruebas de penetración; adicionalmente se atenderán las solicitudes del cliente respecto a su superficie de ataque.

Como Attack Surface Analyst Intern, realizare las funciones de asistir a los miembros del equipo de Inteligencia de Superficies de Ataque con las diferentes actividades de administración de la superficie de ataque de los clientes asignados, completando tareas delegadas para habilitar el trabajo del equipo de Operación de Pruebas de Penetración o responder directamente a una necesidad del cliente, y realizando tareas de automatización.

1.5 Entregables

Los entregables que produciré en el proyecto serán notificaciones y reportes respecto al descubrimiento y validación de superficies de ataque pertenecientes al cliente, notificaciones en respuesta a necesidades del cliente, y contribuciones a tareas de automatización.

Los entregables que produciré personalmente para el Proyecto de Aplicación Personal serán documentos y presentaciones en video o en vivo que servirán para planear y comunicar mi aprendizaje durante el proyecto.

1.6 Involucrados

Los interesados en los resultados del proyecto serán:

- Clientes asignados
- Líder de analistas de Inteligencia de Superficies de Ataque
- Miembros del equipo de trabajo
- Equipo de analistas de Inteligencia de Superficies de Ataque
- Equipo de operadores de Pruebas de Penetración
- Intern de Inteligencia de Superficies de Ataque

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

El proceso de inicio determina la propuesta del proyecto y los objetivos, los cuales son principalmente finalizar la habilitación de interns para expandir la capacidad de operación de los servicios de la compañía. El proceso de planificación establece las actividades necesarias para lograr el objetivo definido, tomando en cuenta la interacción con el equipo de trabajo. Durante el proceso de ejecución del proyecto se lleva a cabo las actividades previamente establecidas para los participantes del proyecto. Durante el proceso de seguimiento y control se aseguran los objetivos del proyecto mediante actividades de seguimiento, contando con los miembros del equipo participante en el proyecto. En el proceso de cierre se evalúan los resultados obtenidos contra los objetivos establecidos y se finaliza el proyecto.

2.2 Sustento Teórico y Metodológico

El procedimiento para la realización del proyecto ha sido desarrollado por la empresa, abarca procesos de mentoría, entrenamiento, y delegación de tareas en el equipo de trabajo. Se han realizado modificaciones a un procedimiento previamente utilizado para la integración de nuevos miembros al equipo de trabajo, con el fin de adaptarlo para su utilización con interns.

2.3 Descripción del Proyecto

La secuencia de procesos que son realizados por el equipo de Inteligencia de Superficies de Ataque según su orden de realización es: el descubrimiento de la superficie de ataque, la validación de la superficie de ataque, la identificación de posibles vulnerabilidades, y la depuración de superficie de ataque e identificación de vulnerabilidades concretas.

El proyecto se desarrolla de manera iterativa, con cada iteración se obtiene mayor control sobre la superficie de ataque del cliente mediante la administración y validación, y el equipo de Inteligencia de Superficies de Ataque continúa desarrollando sus habilidades para realizar las tareas de manera más eficiente y efectiva. Mediante esta iteración se habilita a los interns para obtener las habilidades necesarias para realizar las actividades requeridas.

El proyecto es clasificado como de entrega continua de seguridad a la ofensiva, se habilita a los interns a realizar actividades con el objetivo de la protección de superficies de ataque dinámicas y la entrega al cliente del nivel de servicio estipulado. Los recursos utilizados para el proyecto son plataformas y herramientas desarrolladas dentro de Bishop Fox para el servicio de Cosmos, herramientas de

pruebas de penetración y descubrimiento de superficies de ataque de fuente abierta y propietarias, y recursos de aprendizaje. La mayoría del trabajo es realizado de manera remota mediante equipo de cómputo.

El alcance de mi proyecto educativo contempla las siguientes competencias a desarrollar: investigación de fuentes abiertas, manejo de herramientas, automatización, interacción con el cliente, y colaboración,

No.	Competencia	Nivel Adquirido al Inicio	Nivel Objetivo al final PAP	Objetivo final PAP	Prior
1	Investigación de fuentes abiertas	3	4	4	A
2	Manejo de herramientas	3	4	5	A
3	Automatización	1	2	3	A
4	Interacción con el cliente	2	3	3	M
5	Colaboración	2	3	2	M

2.4 Plan de Trabajo

	Actividad	Fecha Inicio	Fecha Termino	Dias habiles	Dependencias
1	Orientacion	15/Agosto	19/Agosto	5	
1.1	Setup				
2	Hands-on	22/Agosto	25/Noviembre	70	1
2.1	Descubrimiento de superficies de ataque				
2.1.1	Administracion de superficies de ataque				
2.1.2	Validacion de superfcies de ataque				
2.2	Atencion a solicitudes del cliente				
2.3	Desarrollo de automatizacion de analisis				

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	Investigacion de fuentes abiertas																							
1.1	Conocer y utilizar herramientas y tecnicas para el descubrimiento de superficies de ataque (dominios, subdominios, y direccionamiento)	Autoestudio / Tutoria		20	22/Agosto	16/Septiembre																		
1.2	Conocer y utilizar herramientas y tecnicas para el descubrimiento de vulnerabilidades y filtraciones	Autoestudio / Tutoria	1.1	40	19/Septiembre	11/Noviembre																		
2	Manejo de herramientas																							
2.1	Estudio de herramientas especializadas propietarias	Tutoria		20	22/Agosto	16/Septiembre																		
2.2	Estudio de herramientas especializadas de fuente abierta	Curso en linea		30	19/Septiembre	28/Octubre																		
3	Automatizacion																							
3.1	Estudiar la automatizacion de actividades realizada por el equipo	Autoestudio / Tutoria		20	19/Septiembre	14/Octubre																		
3.2	Realizar automatizaciones propias	Autoestudio / Tutoria	3.1	30	17/Octubre	25/Noviembre																		
4	Interaccion con el cliente																							
4.1	Estudio de estilo de comunicacion realizado por el equipo	Autoestudio / Tutoria		10	22/Agosto	2/Septiembre																		
4.2	Realizar control de calidad	Autoestudio / Tutoria	4.1	30	5/Septiembre	14/Octubre																		
5	Colaboracion																							
5.1	Atender y estudiar la participacion en los canales de comunicacion del equipo	Autoestudio		10	22/Agosto	2/Septiembre																		
5.2	Conocer y estudiar la colaboracion en la documentacion para el equipo	Autoestudio / Tutoria		10	5/Septiembre	16/Septiembre																		

2.5 Equipo de Trabajo

<i>Rol</i>	<i>Responsabilidad</i>	<i>Nombre (opcional)</i>
<i>Líder de analistas</i>	<i>Asignación de equipos</i> <i>Asignación de clientes</i>	<i>Attack Surface Analyst Team Lead</i>
<i>Analista</i>	<i>Manejo de amenazas</i> <i>Descubrimiento de superficies de ataque</i> <i>Atención a solicitudes del cliente</i> <i>Validación de superficies de ataque</i> <i>Desarrollo de automatización de análisis</i>	<i>Attack Surface Analyst</i>
<i>Intern</i>	<i>Descubrimiento de superficies de ataque</i> <i>Atención a solicitudes del cliente</i> <i>Validación de superficies de ataque</i> <i>Desarrollo de automatización de análisis</i>	

2.6 Plan de Comunicaciones

<i>Emisor</i>	<i>Mensaje</i>	<i>Receptor</i>	<i>Medio</i>	<i>Frecuencia</i>
<i>Intern</i>	<i>Reporte</i>	<i>Líder de equipo</i>	<i>Plataforma y video conferencia</i>	<i>d</i>
<i>Intern</i>	<i>Reporte</i>	<i>Líder de analistas</i>	<i>Plataforma</i>	<i>s</i>
<i>Intern</i>	<i>Informacion</i>	<i>Líder de analistas</i>	<i>Videoconferencia</i>	<i>2s</i>
<i>Estudiante</i>	<i>Documento</i>	<i>Profesor PAP</i>	<i>Plataforma</i>	<i>m</i>
<i>Estudiante</i>	<i>Documento</i>	<i>Profesor PAP</i>	<i>Videoconferencia</i>	<i>m</i>

2.7 Plan de Calidad

<i>Emisor: Quién Entrega</i>	<i>Entregable: Qué Entrega (Entregable)</i>	<i>Receptor: Quién recibe o Inspecciona</i>	<i>Criterios: Condiciones de Aceptación</i>	<i>Siguiente paso. Cuando se Autoriza.</i>
<i>Intern</i>	<i>Reporte</i>	<i>Analista</i>	<i>Cumple procedimiento y/o realiza necesidad del cliente</i>	<i>Reporte a cliente y/o seguimiento por el equipo de Operación de Pruebas de Penetración</i>

2.8 Seguimiento y Control.

Se reporta diariamente lo que se planea realizar durante el día de trabajo y lo que se realizó el día previo de manera escrita, posteriormente se reporta al líder del equipo de manera oral en una videoconferencia que abarca a todos los miembros del equipo. Se realiza un reporte semanal al líder de analistas de manera escrita,

adicionalmente se realiza una videoconferencia uno a uno con el líder de analistas cada dos semanas.

Se entrega un avance o versión final del documento a redactar para su revisión por el profesor PAP, posteriormente se tiene una sesión de revisión uno a uno o grupal por medio de una videoconferencia y se determina los cambios a realizar en el documento para su posterior entrega o evalúa la entrega.

2.9 Cierre del Proyecto

La evaluación y retroalimentación final se realiza de manera escrita, siendo proporcionada por el líder de analistas, y pudiendo ser discutida durante una de las videoconferencias uno a uno que se encuentran agendadas paralelamente al periodo de cierre del Proyecto de Aplicación Personal.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

Durante mi participación en el proyecto produje principalmente reportes respecto al descubrimiento y validación de la superficie de ataque, contribuciones al histórico de la superficie de ataque de los clientes asignados y a tareas de automatización, y notificaciones en respuesta a necesidades del cliente.

3.2 Estimación del Impacto

Los reportes respecto al descubrimiento y validación de la superficie de ataque producidos durante el proyecto y las notificaciones en respuesta a necesidades del cliente contribuyen a la habilitación de la realización de trabajo de pruebas de penetración y la entrega al cliente del nivel de servicio estipulado. Mis contribuciones al histórico de la superficie de ataque de los clientes asignados y a tareas de automatización son utilizadas para la continuidad de actividades que realiza el equipo de Inteligencia de Superficies de Ataque parte del servicio de Cosmos, aumentando la eficiencia y efectividad del equipo, y por lo tanto, del servicio.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

Las competencias técnicas más importantes directamente relacionadas a la seguridad informática que desarrolle durante el proyecto fueron la investigación de fuentes abiertas y la automatización de tareas para el descubrimiento de vulnerabilidades. Otras competencias técnicas genéricas que desarrolle fueron el manejo de herramientas diversas que son útiles para cualquier ámbito en el que se trabaje con sistemas computacionales. La principal competencia suave que desarrolle durante el proyecto fue la comunicación tanto con el cliente como con mis compañeros de trabajo.

Mis principales aprendizajes sobre el contexto sociopolítico y económico dentro del campo de la seguridad informática fueron que las problemáticas observadas de manera global afectan las tareas que se desarrollan profesionalmente, algunas de estas problemáticas observadas fueron guerras, protestas, y liberación inesperada de vulnerabilidades.

Los principales saberes adquiridos durante mis estudios universitarios que fueron puestos a prueba fueron los conocimientos básicos para el trabajo con servicios y sistemas conectados a internet, lo cual es crucial para actividades del campo de la seguridad informática.

Durante el desarrollo de este proyecto tuve que priorizar tareas y realizar manejo del tiempo dedicado a cada una, por lo tanto considero que puedo trabajar con proyectos que requieran planeación y priorización de mi parte.

4.2 Aprendizajes Sociales

Al contribuir a la protección de la superficie de ataque del cliente, no solo se mantiene la seguridad informática para el cliente, sino para todas las personas que utilizan sus servicios. Mi equipo de trabajo fue responsable de realizar trabajo en herramientas libremente distribuidas durante momentos de crisis para mantener la seguridad informática de todo el mundo, no solo de los clientes asignados. Al habernos enfrentado como equipo y como servicio a un mayor número de situaciones de crisis derivadas de situaciones geopolíticas durante este periodo, pude tener un cambio de perspectiva respecto a cómo el trabajo que realizamos se ve afectado por la realidad cambiante de diversas partes del mundo.

Al formar parte del grupo de empleados de origen mexicano dentro de los equipos que forman el servicio Cosmos de Bishop Fox, contribuí a la expansión de la

compañía dentro del país. Adicionalmente participe en actividades de divulgación y fomento de la seguridad informática en México con miembros de mi equipo.

4.3 Aprendizajes Éticos

Al encontrarme en el segundo periodo de internship con la compañía, se me dio mas acceso a infraestructura y activos relacionados al trabajo a realizar con el cliente, por lo tanto tuve que tomar decisiones respecto a las acciones que tomaría con este nuevo nivel de responsabilidad. Las consecuencias de estas decisiones repercutieron directamente en el cliente, por lo que fue de suma importancia realizar deliberaciones al respecto y solicitar ayuda cuando fue necesario.

Durante el proyecto resulto necesario entender la importancia de la informacion con la que se trata al realizar tareas de seguridad informática y contar con una ética y sentido de responsabilidad que se alinea con lo que la compañía espera.

Después de realizar este proyecto, pudiendo hablar con mis compañeros de trabajo, he identificado el camino que busco tomar en cuanto a mi profesión, pues he solidificado mi decisión de especializarme en el ámbito de inteligencia y análisis dentro de Bishop Fox.

4.4 Aprendizajes Personales

Las actividades realizadas durante este proyecto me han ayudado a identificar de manera más objetiva el nivel de mis habilidades actuales y los puntos de mejora que será necesario tratar para continuar con mi desarrollo profesional y personal.

Al formar parte de un equipo conformado por personas provenientes de diferentes países del mundo con experiencias laborales y educativas diferentes antes de formar parte del equipo, tuve la oportunidad de colaborar y convivir buscando una meta en común, formando parte de un equipo en el que todos los miembros participan de manera equitativa. Al relacionarme con mis compañeros de equipo pude evaluar cuales habilidades me gustaría desarrollar a futuro y como estas pueden ser útiles para mi desarrollo profesional.

4.5 Tareas Aprendidas

El principal factor de éxito para los resultados del proyecto fue el contar con la disposición de todos los miembros del equipo para responder preguntas y dar tutorías, lo cual permitió poder realizar las actividades del proyecto por mí misma, pero contando con apoyo en caso de necesitarlo. Otro factor importante fue el contar con una comunicación abierta con el líder de equipo, al cual pude hacerle preguntas y hablar sobre la realización del trabajo.

Una actitud personal que resulto necesaria para el desarrollo del proyecto fue la iniciativa propia, durante el proyecto fue necesario el demostrar mi iniciativa y ofrecirme a realizar trabajo que previamente no había realizado por mi misma, obteniendo mas responsabilidades dentro de las actividades diarias de trabajo a realizar.

4.6 Desarrollo Profesional

1. Las tareas tecnológicas en las que más me interesa desarrollarme son tareas de análisis, monitoreo, y detección, por lo tanto los proyectos en los que me gusta trabajar son proyectos de inteligencia de fuentes abiertas y detección de vulnerabilidades.
2. El área tecnológica en la que me desarrollo con mayor destreza es el área de la seguridad informática.
3. Las áreas con mayor crecimiento dentro de la seguridad informática son los servicios de monitoreo continuo, evaluación de seguridad, y administración de superficies de ataque, los cuales incluyen tareas de inteligencia y detección de vulnerabilidades.

Durante la realización de este proyecto continúe con el desarrollo de las habilidades necesarias para obtener un puesto en el área de inteligencia enfocada a las superficies de ataque, tomando en cuenta los esfuerzos realizados previamente, alcanzando el perfil necesario para obtener un puesto especializado en una compañía líder en seguridad informática. Adicionalmente, el área de la seguridad informática en general ha presentado un alto crecimiento, tendencia que continuara durante los años próximos.

Actualmente ya he completado mi primer periodo como intern dentro de Bishop Fox, comenzando el desarrollo de mis habilidades en las áreas necesarias para mi objetivo final. Terminare el segundo periodo como intern dentro de Bishop Fox, estando lista para adoptar el puesto objetivo final de manera parcial. Finalmente pasare del puesto objetivo parcial al final.

La razón principal para desarrollarme para la posición que he escogido como objetivo final es el poder trabajar dentro de una de las ramas de la seguridad informática que más me interesan. Otra razón es que quiero seguir formando parte de Bishop Fox, ya que veo oportunidades de crecimiento dentro de la compañía y he obtenido una gran cantidad de conocimiento en un corto tiempo gracias a la manera en la que se maneja el trabajo dentro de ella.

5. Conclusiones

El continuar siendo parte de esta empresa, obteniendo experiencia laboral e interactuando profesionalmente con el mundo de la seguridad informática, me ha permitido continuar desarrollando mis habilidades tanto profesionales como personales. Durante la duración del proyecto continúe interactuando con los miembros de mi equipo y conociendo a miembros que se integraron más adelante, pudiendo ver las diferentes formas en las que se puede desarrollar un rol en áreas de la seguridad informática relacionadas a la inteligencia. Debido a que es mi segundo periodo de internship con Bishop Fox, pude realizar una mayor cantidad de trabajo de manera independiente, experimentando integralmente el cómo es realizar el trabajo del puesto para el que busco prepararme, en mi caso para el rol de analista de superficie de ataque.

Ha sido importante realizar la documentación de mi experiencia y reflexiones durante este proyecto, ya que mediante esta documentación será posible comunicar lo que se ha realizado y el efecto que ha tenido tanto de manera profesional como personalmente.

Este ha sido un periodo de transición para la compañía, por lo que pude experimentar por primera vez el movimiento que esto conlleva, presenciando la creación y desaparición de equipos, y cambios en la conformación de equipos. Esto me resulto importante porque es necesario contar con un nivel de flexibilidad al trabajar dentro de empresas en crecimiento.

Al finalizar el proyecto obtuve los objetivos esperados, obtuve los conocimientos y habilidades necesarios para desarrollar las tareas, pero más allá de ello obtuve experiencia trabajando de manera conjunta y experimenté un más alto nivel de responsabilidad respecto a un trabajo dentro de la industria con la que se encuentra relacionada mi carrera universitaria, preparándome para los siguientes pasos a tomar tras la conclusión de mis estudios.