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: ICB, Salvador Rodríguez Arrieta

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

Tlaquepaque, Jalisco, mayo 2024

**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

En mi rol como parte del departamento de Cosmos, me desempeño como operador adversarial. Mis responsabilidades incluyen identificar y explotar vulnerabilidades en la superficie de ataque de nuestros clientes, elaborar informes detallados sobre dichas fallas, brindar apoyo a los clientes en la resolución de los problemas identificados, llevar a cabo reuniones con ellos y desarrollar herramientas para el equipo. Con una trayectoria de cinco años en la industria tecnológica, de los cuales dos han sido enfocados específicamente en ciberseguridad ofensiva, el propósito de mi proyecto es perfeccionar las habilidades más especializadas que me permitan desempeñar un papel único dentro del equipo.

Adicionalmente, aplicaré los conocimientos adquiridos en el PAP anterior cursado, lo que me brindará una base sólida para afrontar los desafíos que se presenten en este proyecto y perseguir mi objetivo de crecimiento profesional. La combinación de mi experiencia previa y las competencias desarrolladas durante el PAP me permitirán abordar de manera efectiva las tareas de mi puesto, aportando valor tanto a nuestros clientes como al equipo en general. Este proyecto representa una oportunidad para seguir creciendo profesionalmente y consolidarme como un experto en ciberseguridad ofensiva.

# 1. Introducción

## 1.1 Antecedentes

Bishop Fox es una empresa líder a nivel mundial en el campo de la ciberseguridad ofensiva. La empresa realiza pruebas de seguridad en diversas tecnologías como aplicaciones móviles, la nube y tecnologías web, entre otras. Ofrece servicios de consultoría y de pruebas de penetración continuas. Sus clientes son empresas de todas las industrias, desde alimenticias y manufactura, hasta médicas y bancarias, a nivel mundial.

Su misión y valores apuntan hacia el mismo lado, hacia la excelencia. Su objetivo es ser un referente en cuestión de calidad, investigación y contribuciones a la comunidad. Sus valores reflejan esto, enfocándose en la constante mejoría personal y del equipo y sobre el ambiente que se debe de crear para conseguirlo.

## 1.2 Justificación

El enfoque de Bishop Fox como una empresa dedicada íntegramente a la seguridad ofensiva la convierte en una organización ideal para especializarme y crecer en este campo. Su equipo está compuesto por profesionales de renombre internacional, con una amplia trayectoria en proyectos, investigaciones y logros destacados, lo que los convierte en mentores excepcionales.

Invertiré la totalidad de las veinte horas del PAP en este proyecto, ya que mi prioridad es adquirir experiencia práctica. Aunque ya cuento con un dominio en las diversas responsabilidades que asumiré, mi objetivo es adquirir nuevas responsabilidades y crecer en mi posición.

Para facilitar mi desarrollo, se me ofrecerán diversas oportunidades, como la opción de dedicar cuatro horas semanales a autoestudio. Asimismo, mantendré reuniones semanales con mi manager, en las que podré plantear todas mis dudas y solicitar orientación.

## 1.3 Objetivos

El objetivo de la empresa es ofrecer oportunidades de crecimiento para nuevos profesionistas y poder apoyar a sus empleados que aún son estudiantes para poder completar sus objetivos profesionales.

Mis objetivos serán el desarrollar las habilidades de un operador III, hacer investigación de nuevas técnicas de ataques en la nube de AWS y LLMs, así como prepararme para obtener la certificación OSCP. Aprenderé también habilidades no técnicas, como el trato con clientes y las habilidades de comunicación en equipos remotos.

## 1.4 Contexto

Como miembro del departamento de Cosmos, asumiré el rol de operador adversarial de medio tiempo. Cada cliente tiene su propio proyecto dentro del departamento, con una duración que oscila entre uno y tres años. Estos proyectos se centran en realizar pruebas de penetración continuas, cuyo objetivo es someter a los clientes a ataques constantes para identificar vulnerabilidades de seguridad y ayudarlos a solucionarlas antes de que puedan ser explotadas por actores malintencionados.

Mis responsabilidades dentro de estos proyectos incluirán detectar y aprovechar fallos de seguridad en la infraestructura y superficie de ataque de nuestros clientes, elaborar y presentar informes detallados, mantener comunicación con los clientes a través de llamadas, atender sus consultas específicas sobre nuestro trabajo, comprobar que las vulnerabilidades hayan sido resueltas y crear herramientas para el resto del equipo. Todas estas tareas forman parte del área operativa.

## 1.5 Inventario de Competencias

| *No.* | *Competencia* | *Req* | *Adq* | *GAP* | *Obj* | *Prior* |
|---|---|---|---|---|---|---|
| *1* | Pruebas de Seguridad en LLMs | | | | | |
| *1.1* | *Identificación de LLMs en aplicaciones web* | *3* | *1* | *2* | *3* | *3* |
| *1.2* | *Identificar vulnerabilidades en LLMs en aplicaciones web* | *3* | *0* | *3* | *3* | *3* |
| *2* | Comunicación en inglés | | | | | |
| *2.1* | *Comunicación escrita en inglés* | *5* | *5* | *0* | *3* | *5* |
| *2.2* | *Comunicación oral en inglés* | *5* | *5* | *0* | *3* | *5* |
| *3* | Comunicación con clientes | *5* | *4* | *1* | *5* | *2* |
| *4* | Uso del C2 Sliver | *3* | *0* | *3* | *3* | *4* |
| *5* | Pruebas de penetración en redes Internas | *5* | *3* | *2* | *5* | *1* |

## 1.6 Plan Educativo

| | | | |
|---|---|---|---|
| Materia | PAP1- DESI | Semestre | 2024V |
| Profesor | Juan Manuel Islas | Horario: | Lun-Jue 16-18 |

| | | | |
|---|---|---|---|
| Alumno: | Salvador Rodríguez Arrieta | Carrera: | ICB |
| PAP: | PROGRAMA DE LA INDUSTRIA DE ALTA TECNOLOGIA II | | |
| Empresa: | Bishop Fox | | |

**Plan de Actividades**

| No. | Actividad Educativa | Tipo Actividad | Total Hrs | Fecha Inicio | Fecha Termino | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | **Comunicación con Clientes** | Práctica | 10 | 20/05 | 13/07 | | | | | | | | |
| | | | | | | | | | | | | | |
| 1 | **Pruebas de seguridad en llms** | | | | | | | | | | | | |
| 1.1 | Identificación de LLMs en aplicaciones web | Práctica | 5 | 27/05 | 7/6 | | | | | | | | |
| 1.2 | Identificar vulnerabilidades en LLMs en aplicaciones web | Autoestudio | 10 | 7/6 | 21/06 | | | | | | | | |
| | | | | | | | | | | | | | |
| 4 | **Uso del C2 Sliver** | Práctica | 5 | 24/06 | 13/05/24 | | | | | | | | |
| 5 | **Pruebas de Penetración en redes internas** | Autoestudio | 50 | 20/05 | 05/07 | | | | | | | | |

## 1.7 Entregables

El principal entregable que se creará, son los reportes de vulnerabilidades de los clientes. Estos se redactarán de forma diaria, dependiendo del resultado del trabajo de ese día. De igual manera, como entregables más técnicos, se realizará documentación y código, en forma de herramientas para el resto del equipo. Para finalizar, para las juntas con los clientes se crearán presentaciones conteniendo información relevante según su proyecto.

## 1.8 Involucrados

- Manager
- Operadores
- Analistas
- Clientes
- Encargados de cuentas de clientes

# 2. Desarrollo del Proyecto PAP

## 2.1 Administración del Proyecto

La administración del proyecto se lleva a cabo siguiendo metas definidas por el líder técnico del equipo, junto a los supervisores del equipo de clientes. Durante el inicio del proyecto de cada cliente, se tiene una reunión donde se expresan las metas del proyecto y las reglas a seguir para cada cliente. En la planificación, hay varias juntas que se tienen de forma semanal, con diferentes equipos involucrados; como con el equipo de ingeniería. La ejecución, seguimiento y control, ocurren directamente con el equipo de operadores. Aquí, se nos da una planeación de ejecución semanal, donde se cubren las labores a realizar.

Mis compañeros operadores, dan el seguimiento y control. El seguimiento ocurre en dos juntas semanales y el control ocurre al terminar cada caso. El proceso de control depende del día. Cada día se asigna una persona diferente del equipo a este proceso y se encargan de realizar un control del proceso y verificar los entregables de cada cliente. El cierre es realizado por el líder técnico y los supervisores del equipo de clientes.

## 2.2 Sustento Teórico y Metodológico

La metodología utilizada es un workflow propio llamado investigaciones. Las investigaciones inician con un analista, que realiza los procesos de rediscovery y triage. A partir de los resultados de estos procesos, se crean casos. Los operadores investigamos estos casos, en búsqueda de vulnerabilidades.

Al finalizar un caso, los operadores redactamos un documento llamado finding, donde se le explica al cliente lo que se encontró como resultado de la investigación. Este suele incluir una explicación detallada de la vulnerabilidad que se encontró, como se explotó y los resultados de explotarla, así como recomendaciones para solucionarla.

## 2.3 Descripción del Proyecto

Mi proyecto es parte de las operaciones de negocio de la organización. Mis labores son las de un Operador Adversarial. El equipo de Cosmos, es un departamento de Bishop Fox, que ofrece servicios continuos, es decir, ofrece proyectos de duración de varios años a sus clientes. Nuestro trabajo es ayudar a los clientes a identificar fallas en su seguridad, para que puedan solucionarlas. Mi labor en el proyecto es cubrir las responsabilidades de un operador, por lo que realizo investigaciones, redacto hallazgos y los reporto a los clientes. Todo siendo parte de las operaciones del equipo.

La secuencia del proceso es que primero el equipo de analistas identifica los activos de los clientes. Posteriormente, los activos son enviados a los operadores para que podamos identificar fallos de seguridad en ellos. Una vez que se investigó un activo, se redacta un reporte que es el compartido con el cliente, el cual es el primer entregable. El segundo entregable, es una reunión de seguimiento que se hace cada tres meses con los clientes, donde se expone los resultados y se resuelven posibles dudas.

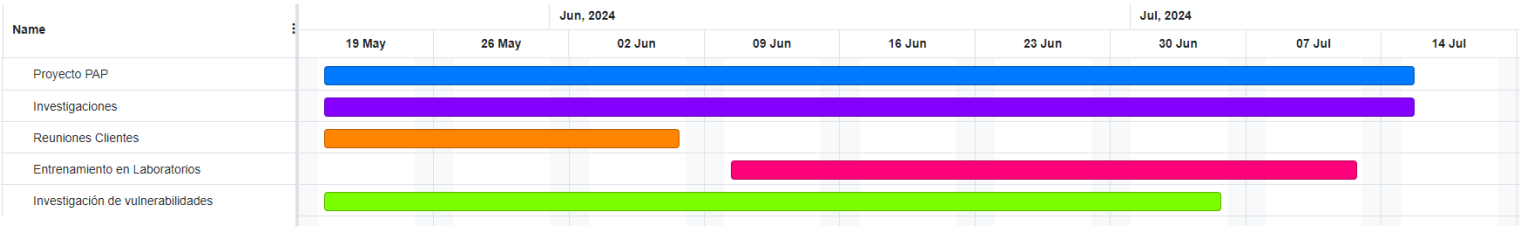
Los recursos tecnológicos más importantes para producir los entregables de la organización son:

- La plataforma de Cosmos
- Github
- AWS

## 2.4 Tipo de Proyecto

El ciclo de vida del proyecto no corresponde a uno conocido, debido a que es propio, desarrollado por la organización. Sin embargo, se basa en la metodología ágil y hay algunas similitudes con otras, como, por ejemplo, el uso de daily standups, all hands y el uso de un backlog.

## 2.5 Plan de Trabajo




## 2.6 Equipo de Trabajo

| *Rol* | *Responsabilidad* | *Nombre (opcional)* |
|---|---|---|
| Líder Técnico | Establecer planes de trabajo para el equipo<br><br>Resolver problemas técnicos o de procesos<br><br>Mantener la comunicación entre todas las demás partes del equipo | |
| Operador (Alumno) | Realizar investigaciones en los activos de los clientes<br><br>Comunicar hallazgos<br><br>Resolver dudas de clientes respecto a los reportes | |
| Analista | Identificar los activos de los clientes<br><br>Comunicar hallazgos<br><br>Resolver dudas del equipo y los clientes sobre la plataforma | |
| Supervisor de clientes | Mantener la comunicación con los clientes<br><br>Comunicar las necesidades de los clientes con el resto del equipo<br><br>Resolver conflictos con los clientes | |

## 2.7 Plan de Comunicaciones

| *Emisor* | *Mensaje* | *Receptor* | *Medio* | *Frecuencia* |
|---|---|---|---|---|
| Alumno | Dudas y avances | Profesor PAP | Video llamada | Mensual |
| Alumno | Reportes | Clientes | Archivo electrónico y video llamadas | Diario |
| Líder técnico | Planificación | Equipos | Video llamadas | Diario |

## 2.8 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.* |
|---|---|---|---|---|
| Operador a cargo de investigación | Reporte | Operador en turno | Lineamientos de reportes de Operadores | Plataforma de Cosmos |
| Operador (Alumno) | Presentación Powerpoint | Líder Técnico | Guía de estilo de Cosmos | Reunión con el cliente |

## 2.9 Seguimiento y Control

El control y monitoreo se hace en una llamada cada viernes, de forma semanal. En esta llamada se revisa el progreso, se hacen modificaciones y se escucha el feedback de ambas partes, para poder mejorar el proyecto y hacer ajustes correspondientes. Esto me ayuda a cumplir mis objetivos del proyecto, porque me permite estar informado para realizar ajustes y poder compartir mis objetivos para que sean tomados en cuenta.

Del lado del proyecto PAP, tengo clases semanales con mi profesor, donde puedo resolver preguntas, pedir apoyo y retroalimentación. Del mismo modo, tengo reuniones mensuales donde se revisa mi progreso y se da retroalimentación directa sobre mi reporte.

# 3. Resultados del Trabajo Profesional

## 3.1 Productos Obtenidos

1. Plantillas de Hallazgos
2. Guías de explotación de vulnerabilidades
3. Findings
4. Diapositivas para clientes
5. Programas para automatizar tareas

## 3.2 Estimación del Impacto

El impacto de los entregables producidos ha sido significativamente alto. Estos productos y servicios han permitido que empresas internacionales implementen medidas robustas de protección, protegiendo la seguridad y bienestar de sus clientes y empleados. La trascendencia de este trabajo se refleja en la capacidad mejorada de estas organizaciones para enfrentar amenazas y mantener la confianza en un entorno empresarial cada vez más complejo y globalizado.

# 4. Reflexiones del alumno

## 4.1 Aprendizajes Profesionales

1. Trato con clientes
2. Explotación avanzada en entornos de Active Directory
3. Explotación avanzada en entornos Web

## 4.2 Aprendizajes Sociales

La contribución a la sociedad es fundamental y de gran alcance. Principalmente por salvaguardar la confidencialidad de la información personal, protegiendo así la privacidad de los individuos. Además, el proyecto juega un papel crucial en garantizar la continuidad operativa de sistemas críticos, incluyendo los sectores de salud, finanzas y energía. Esta labor es esencial para mantener la estabilidad y el funcionamiento de servicios vitales para la sociedad, asegurando que la infraestructura crítica permanezca resiliente frente a posibles amenazas y disrupciones.

## 4.3 Aprendizajes Éticos

En mi experiencia PAP, he encontrado una fuerte concordancia entre mis valores morales y el sentido social de la empresa huésped, particularmente en lo que respecta a la protección de información confidencial de las personas. Esta experiencia me ha hecho más consciente de las implicaciones éticas en mi profesión, especialmente en cuanto a la responsabilidad de proteger datos sensibles y mantener la confianza pública en los sistemas tecnológicos.

## 4.4 Aprendizajes Personales

Me siento más seguro en mis habilidades y decisiones, especialmente al enfrentar desafíos complejos. Esta experiencia ha contribuido a mi madurez, ayudándome a reconocer mis fortalezas y áreas de mejora en el campo de la ciberseguridad. Además, trabajar en un entorno diverso me ha enseñado a valorar diferentes perspectivas y a colaborar eficazmente con personas de distintos orígenes, mejorando mi capacidad para convivir en la pluralidad y apreciar la diversidad en el ámbito profesional.

## 4.5 Tareas Aprendidas

El éxito del proyecto se debió principalmente a tres factores clave. Una comunicación eficaz y constante entre todos los miembros del equipo, un fuerte espíritu de colaboración y apoyo mutuo, y el acceso a numerosos recursos para resolver dudas y superar obstáculos. Esta combinación de elementos creó un ambiente propicio para la innovación y la resolución efectiva de problemas, permitiéndonos alcanzar nuestros objetivos de manera eficiente y exitosa.

## 4.6 Desarrollo Profesional

1. Tareas tecnológicas de mayor interés:

a) Pentesting

b) Red Teaming

c) Security Content engineering

2. Áreas tecnológicas de mayor destreza:

a) Pentesting web

b) Cloud pentesting

c) Internal Pentesting

3. Áreas de mercado con mayor crecimiento:

a) Seguridad de la información

b) Inteligencia artificial y aprendizaje automático

c) Computación en la nube

Para alcanzar mi posición objetivo, planeo: profundizar mis conocimientos en técnicas avanzadas de pentesting, participar en competencias de captura la bandera (CTF), y buscar certificaciones especializadas en seguridad ofensiva.

Mi plan de desarrollo profesional a mediano plazo implica: mantenerme al día con las últimas vulnerabilidades y técnicas de explotación, participar en conferencias de seguridad, y contribuir a la comunidad de seguridad compartiendo conocimientos y herramientas.

Las tendencias del mercado incluyen: aumento en la demanda de profesionales de seguridad ofensiva, integración de IA en herramientas de pentesting, y un enfoque creciente en la seguridad en la nube. El ambiente laboral se está volviendo más flexible, con equipos distribuidos globalmente.

Me interesa participar en proyectos de red teaming para grandes corporaciones o infraestructuras críticas, ayudando a fortalecer sus defensas mediante simulaciones realistas de ataques.

Los factores que justifican invertir en este sector son: la constante evolución de las amenazas cibernéticas, la oportunidad de estar siempre a la vanguardia tecnológica, y la satisfacción de contribuir directamente a mejorar la postura de seguridad de organizaciones críticas.

## 5. Conclusiones

Documentar mis experiencias, aprendizajes y reflexiones durante el PAP ha sido invaluable, permitiéndome consolidar conocimientos, identificar áreas de mejora y reconocer mis logros. Este ejercicio es una herramienta muy útil para la presentación formal de mi experiencia, destacando los aspectos más relevantes de mi crecimiento profesional. Durante el proyecto, enfrenté situaciones imprevistas que resultaron en lecciones significativas, como la importancia de la comunicación efectiva con equipos no técnicos.

Mi grado de satisfacción al término de esta etapa es alto, ya que el PAP representó un reto considerable que exigió un esfuerzo sustancial, pero los resultados obtenidos superaron mis expectativas.