

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: ICIB, David Córdova Rosendo

Profesor PAP: Juan Manuel Islas Espinoza, PMP®

Tlaquepaque, Jalisco, mayo 2025.

ÍNDICE

REPORTE PAP	2
Presentación Institucional de los Proyectos de Aplicación Profesional	2
Resumen.....	3
1. Introducción	4
1.1 Antecedentes	4
1.2 Justificación	5
1.3 Objetivos	6
1.4 Contexto.....	6
1.5 Inventario de Competencias	7
1.6 Plan Educativo	7
1.7 Entregables.....	8
1.8 Involucrados.....	8
2. Desarrollo del Proyecto PAP.....	9
2.1 Administración del Proyecto.....	9
2.2 Sustento Teórico y Metodológico	9
2.3 Descripción del Proyecto.....	9
2.4 Plan de Trabajo	10
2.5 Equipo de Trabajo	11
2.6 Plan de Comunicaciones	11
2.7 Plan de Calidad	12
2.8 Seguimiento y Control	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.....	15
4.3 Aprendizajes Éticos	15
4.4 Aprendizajes Personales	16
4.5 Tareas Aprendidas.....	16
5. Conclusiones.....	17

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 objetivo de este trabajo es poder compartir el alcance de la ciberseguridad en el mundo real. A lo largo de este semestre voy a estar trabajando en conjunto con el equipo de ciberseguridad de ITLegalServices en donde podré aprender mucho de actividades de ciberseguridad en contextos reales, maneras de prevención y sobre todo contribuir con el conocimiento que adquiriré a lo largo de la carrera.

Hoy en día los dispositivos IoT están por todo el mundo, el hecho de que casi cualquier artefacto pueda conectarse a internet y tener ciertas funcionalidades que faciliten las tareas humanas crea un factor de riesgo un poco sutil. Últimamente han surgido muchas empresas de muchas partes del mundo creando estos dispositivos, y por ende, uno no sabe el tipo de software que fue instalado. Es así como la empresa ITLegalServices necesita un equipo de ciberseguridad capacitado para poder identificar que el software instalado no esté contaminado con software malicioso que aprovechan el consumo masivo para infiltrarse en redes, bases de datos o diversos sistemas que estén conectados a la misma red.

1. Introducción

1.1 Antecedentes

Empresa huésped: IT Legal Services

La empresa principalmente se enfoca en ser un despacho especializado en ciberseguridad, combate de delitos tecnológicos y cómputo forense. Se dedican a otorgar servicios de asesoría y representación técnico legal de empresas, instituciones o personas que han sido víctima de delitos tecnológicos en Latino América para dar con los responsables, así como apoyar en la recuperación de activos comprometidos para restablecer las operaciones tecnológicas.

Hoy en día cualquier empresa que use algún tipo de recurso informático necesita sí o sí seguridad informática, por lo que IT Legal Services puede tener diversos tipos de clientes (manufactura, finanzas, servicios, gobierno, mercados locales, globales, etc)

Misión de la empresa:

Proteger a empresas, instituciones y personas contra el cibercrimen mediante soluciones innovadoras en ciberseguridad, análisis forense digital y consultoría en delitos tecnológicos. Se enfocan en garantizar la seguridad de la información y ofrecer respuestas efectivas ante incidentes, contribuyendo a la justicia digital con investigaciones precisas y éticas.

Visión de la empresa:

Ser el despacho líder en ciberseguridad y cómputo forense en Latinoamérica, reconocido por su capacidad para combatir delitos tecnológicos, detectar amenazas y proporcionar evidencia confiable en procesos legales. Buscan ser referencia en innovación, excelencia y seguridad digital en un mundo interconectado.

Valores de la empresa:

Ética y transparencia: Integridad en cada investigación, asegurando el manejo responsable de la evidencia.

Confidencialidad: Protección de la información con altos estándares de seguridad.

Innovación tecnológica: Uso de herramientas y metodologías avanzadas en ciberseguridad y análisis forense.

Compromiso con la justicia: Apoyo en investigaciones con pruebas digitales verificables.

Excelencia profesional: Servicios de alta calidad con expertos certificados.

Responsabilidad social: Promoción de la educación en ciberseguridad para un entorno digital más seguro.

1.2 Justificación

Creo que, con este PAP, me acerco mucho a una rama de la que me gustaría dedicarme profesionalmente algún día. A lo largo de la carrera realizamos varias pruebas de vulnerabilidad o de penetración a sistemas, pero todo era controlado por nosotros, en ambientes seguros y nada que pudiera perjudicar mucho. Sin embargo, con este plan de trabajo que nos otorgó IT Legal Services, me entusiasma poder trabajar con dispositivos que se usan en ambientes de trabajo reales y que nos pueden dar esa parte de la experiencia que nos hizo falta en clases, así como poder trabajar en conjunto con especialistas que me puedan compartir sus vivencias y situaciones en la empresa.

Este proyecto me tomará alrededor de unas 16 horas a la semana, en este momento estoy viendo administración de servidores Linux en una de mis materias y creo que complementa muy bien con los tipos de dispositivos que voy a utilizar, así como todo el conocimiento que adquiriré en materias pasadas me ayudarán a poder completar las actividades asignadas por la empresa de manera satisfactoria.

De momento la empresa me apoyó con 3 dispositivos IoT para realizar las pruebas (Raspberry Pi / ESP32 / Mini PC para monitoreo de tráfico), en las que se le deberán instalar los programas para escaneo de vulnerabilidades o amenazas, también se nos otorgó un curso para poder comprender mejor cómo funcionan los dispositivos IoT, por lo que me será muy útil para poder desarrollar las actividades que se me asignen. Esta línea de negocio me parece interesante, creo que en un futuro todas las empresas van a necesitar ciberseguridad, así de importante como se necesitan abogados, contadores y administradores. Por lo que empezar realizando pruebas de seguridad a dispositivos creo que es una excelente manera de adentrarme a este mundo, puede que se me presenten situaciones que no se me presentaron durante la carrera el cual tomará mucho valor curricular para mí, así como conocimiento profesional, además, me ayudará a poder darme cuenta si este es el tipo de negocio al que me quiero dedicar.

1.3 Objetivos

La empresa se dedica a dar análisis forense y combatir delitos cibernéticos o tecnológicos, así como tratar de recuperar los activos comprometidos en caso de que se tengan que reestablecer dichas operaciones. Durante este proceso, la empresa provee análisis a dispositivos para asegurar que no tengan software malicioso y que todo lo que esté en la red esté 100% controlado por el propietario. Esto me emociona porque las herramientas y metodologías que vea en este PAP serán muy diferentes a las actividades realizadas durante mi carrera, por lo que tendré una perspectiva nueva que me entusiasma aprender.

En este proyecto, se generará un sensor basado en hardware y software que permita el descubrimiento de dispositivos IoT conectados a la red o dentro de un hogar y brindar un semáforo de riesgos de explotación.

1.4 Contexto

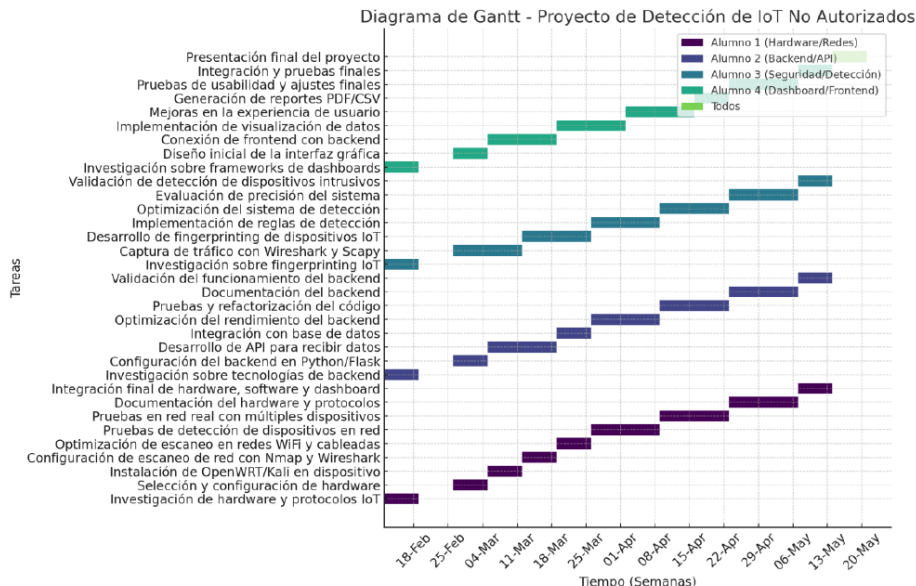
En este caso, toda la empresa se dedica a realizar análisis forense y combatir delitos tecnológicos, sin embargo se va a trabajar en el área de Dirección tecnológica y área de desarrollo de productos en un proyecto creado por el director de TI de dicha empresa (nuestro otro profesor) en donde se enfoque en detectar o descubrir IoTs no autorizados en una red, ya que debido al incremento del ecosistema de dispositivos IoT mediante diversas aplicaciones estos se han vuelto un vector de compromiso en las organizaciones y hogares al carecer en su diseño de medidas de ciberseguridad optimas que eviten ser utilizado como instrumento de ataque. Por lo que junto con el profesor y mis demás compañeros PAP estaremos como interns desarrollando este proyecto, realizaremos funciones distintas como programación a dispositivos móviles, análisis de tráfico en la red y desarrollo backend & frontend para que así estos dispositivos puedan quedar en correcto funcionamiento para futuros clientes en donde se necesite hacer detección de IoTs.

1.5 Inventario de Competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	Manejo eficiente de Kali Linux (Distribución de Linux)	3	3	0	3	A
1.1	Conocimientos de los editores de texto en Linux	3	2	1	3	M
1.2	Uso correcto de las herramientas de scanning	2	3	0	3	A
1.3	Manejo de comandos de hacking	3	3	0	3	A
2	Comunicación en inglés	3	3	0	3	M
2.1	Comunicación escrita en inglés	3	3	0	3	A
2.2	Comunicación oral en inglés	3	2	1	3	M
3	Desarrollo backend y API	3	1	2	3	A
3.1	Implementación del servidor backend	2	1	1	3	A
3.2	Desarrollo de API REST para procesar datos y gestionar bases de datos	2	1	1	3	A
4	Desarrollo frontend y dashboard	3	2	1	3	M
4.1	Diseño e implementación de una interfaz gráfica	3	2	1	2	M
4.2	Diseño de dashboard para visualizar y reportar dispositivos detectados	3	2	1	2	M
5	Redes	3	3	0	3	A
5.1	Configuración de redes para el escaneo de dispositivos	3	2	1	3	A

1.6 Plan Educativo

En este caso, a mi se me asignó ser el Alumno 1 (enfocado a hardware y redes)



1.7 Entregables

De acuerdo con los entregables autorizados para mostrar, nos otorgaron los siguientes:

- Código fuente documentado (Backend, detección de IoTs y dashboard).
- Informe técnico detallado con descripción de arquitectura, metodologías y resultados.
- Dispositivo funcional que pueda detectar IoTs en una red.
- Presentación final con demostración en vivo.

1.8 Involucrados

Los involucrados para este proyecto son mis compañeros de carrera Emiliano Trejo Ríos, Federico Garibay Jiménez y Brenda Marlem Vela Ibarra, a cada uno se le asignara una parte del desarrollo del proyecto, así como se puede ver en la imagen:

Rol	Alumno Asignado	Responsabilidades
Ingeniero de Hardware y Redes	DAVID	Configuración de hardware, instalación de sistemas operativos y configuración de redes para el escaneo de dispositivos.
Desarrollador Backend y API	EMILIANO	Implementación del servidor backend, desarrollo de API REST para procesar datos y gestionar la base de datos.
Especialista en Seguridad y Detección	MARLEM	Implementación de sniffing de tráfico, fingerprinting de dispositivos IoT y detección de amenazas.
Desarrollador Frontend y Dashboard	FEDERICO	Diseño e implementación de una interfaz gráfica para visualizar y reportar dispositivos detectados.

Nuestro asesor de parte de la empresa es el profesor Carlos Eduardo González Durón, el cual ejerce como director de innovación tecnológica y desarrollo de productos en la empresa IT Legal Services, en donde se planea que lo que desarrollemos, se pueda implementar para futuros clientes y que la empresa pueda tener este tipo de servicio disponible.

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

Para la administración del proyecto, de inicio tendremos una sesión con el profesor de parte de la empresa para la explicación sobre de qué se tratará el proyecto y le comentamos de nuestra parte la información que necesitamos para la primera entrega de este reporte.

Después, tuvimos la segunda sesión de planificación con el profesor de la empresa y nos mandó por correo electrónico el plan de actividades y los roles a seguir por cada uno de nosotros durante la ejecución del proyecto. Hablando de esta, comenzamos investigando sobre herramientas de escaneo de vulnerabilidades en Linux para poder entrar en contexto una vez se nos fueran otorgados los dispositivos. Una vez que se nos entreguen, procederemos a realizar las configuraciones correspondientes según nuestro cronograma de actividades. Como seguimiento, el profesor nos hará visitar la empresa para terminar las configuraciones pendientes y asegurarse que todo esté funcionando correctamente para poder tener un buen control. Finalmente, el cierre consistirá en documentar todo el proceso que conllevan las herramientas, su instalación y su funcionamiento con el programa de escaneo que crearemos.

2.2 Sustento Teórico y Metodológico

Como este proyecto es una iniciativa para poder ver el funcionamiento de los dispositivos que configuraremos, nuestra metodología se basará en el libro 'IoT Security Essentials, Student Material – Professional Series' de la editorial 'EC-Council', en donde tendremos como guía para revisar los fundamentos de IoT, redes y comunicaciones y seguridad básica, para que podemos ir conociendo como funcionan estos dispositivos y cómo podríamos escanearlos.

Sin embargo, no se nos especificó una metodología exacta que ya haya sido utilizada por la empresa para específicamente un proyecto de esta especie. Como esto es un proyecto del lado del departamento del profesor y apenas es algo que se piensa implementar, no se ha establecido una metodología fija, aunque se espera que para final de proyecto podamos dejar una nueva creada por nosotros.

2.3 Descripción del Proyecto

Para este proyecto se nos dividirán los roles y actividades entre los 4 alumnos integrantes a este PAP de crear un Sistema de Detección y Descubrimiento de IoTs No Autorizados en una Red. Será una iniciativa nueva de parte del director del departamento de innovación tecnológica y área de desarrollo de productos en donde

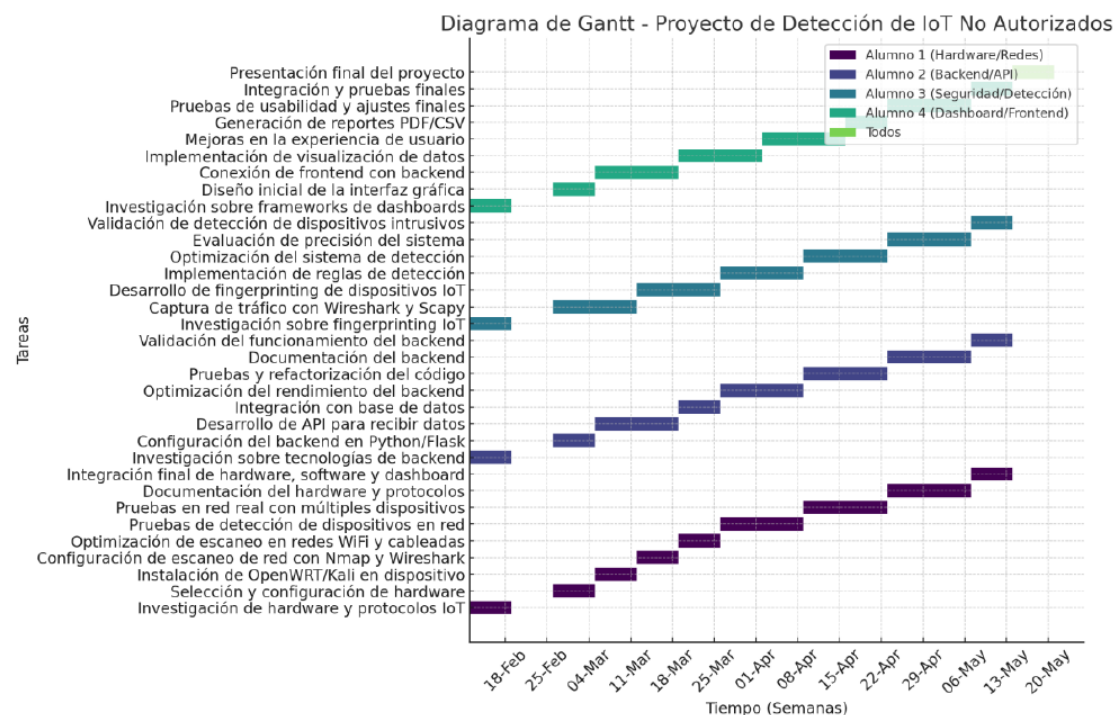
la finalidad es que la empresa pueda tener este nuevo campo o especialidad y se pueda ofrecer que también como parte de sus servicios de prevención de amenazas. Como responsable de la implementación, llevaré a cabo un proceso estructurado que abarca desde la investigación y configuración del hardware hasta la integración final con un dashboard. El trabajo iniciará con una investigación sobre hardware y protocolos IoT, permitiéndome seleccionar y configurar el equipo adecuado. Posteriormente, instalaré sistemas como OpenWRT y Kali Linux en los dispositivos para dotarlos de herramientas avanzadas de análisis de red. Una vez configurado el entorno, procederé a la integración de herramientas como Nmap y Wireshark para el escaneo de la red, asegurando que los dispositivos sean capaces de identificar y analizar patrones de comunicación.

Luego, optimizaré el proceso de escaneo en redes tanto cableadas como inalámbricas para mejorar la precisión y eficiencia en la detección de dispositivos IoT. Con este ajuste, realizaré pruebas de detección en entornos controlados y posteriormente en redes reales con múltiples dispositivos, evaluando la efectividad del sistema en diferentes escenarios.

Tras la fase de pruebas, procederé a documentar el hardware y los protocolos utilizados, generando un registro detallado del proceso. Finalmente, realizaré la integración completa del hardware, software y el dashboard que permitirá visualizar los dispositivos detectados, proporcionando una solución funcional y práctica para la detección de dispositivos IoT no autorizados en la red.

2.4 Plan de Trabajo

En orden alumno 1 al 4: David, Emiliano, Marlem y Federico:



2.5 Equipo de Trabajo

En la tabla se puede encontrar qué alumno es correspondiente a la tabla mencionada en la sección anterior (2.4)

<i>Rol</i>	<i>Responsabilidad</i>	<i>Nombre (opcional)</i>
<i>Líder de proyecto</i>	<i>Supervisar la ejecución y desarrollo de proyecto</i>	<i>Carlos Eduardo González Durón</i>
<i>Ingeniero de hardware y redes</i>	<i>Configuración de hardware, instalación de sistemas operativos y configuración de redes para el escaneo de dispositivos</i>	<i>David Córdova Rosendo (alumno 1)</i>
<i>Desarrollador Backend y API</i>	<i>Implementación del servidor backend, desarrollo de API REST para procesar datos y gestionar la base de datos</i>	<i>Emiliano Trejo Ríos (alumno 2)</i>
<i>Especialista en seguridad y detección</i>	<i>Implementación de sniffing de tráfico, fingerprinting de dispositivos IoT y detección de amenazas</i>	<i>Brenda Marlem Vela Ibarra (alumno 3)</i>
<i>Desarrollador frontend y dashboard</i>	<i>Diseño e implementación de una interfaz gráfica para visualizar y reportar dispositivos detectados</i>	<i>Federico Garibay Jimenez (alumno 4)</i>

2.6 Plan de Comunicaciones

<i>Emisor</i>	<i>Mensaje</i>	<i>Receptor</i>	<i>Medio</i>	<i>Frecuencia</i>
<i>David Córdova</i>	<i>Reporte PAP</i>	<i>Profesor PAP</i>	<i>Plataforma canvas y sesiones en Microsoft Teams</i>	<i>15 días</i>
<i>David Córdova</i>	<i>Progreso de proyecto</i>	<i>Profesor empresa</i>	<i>Correo electrónico</i>	<i>20 días</i>
<i>David Córdova</i>	<i>Resultados de la configuración de hardware y redes para escaneo de dispositivos</i>	<i>Marlem</i>	<i>Microsoft teams, correo electrónico</i>	<i>10 días</i>

2.7 Plan de Calidad

<i>Emisor: Quién Entrega</i>	<i>Entregable: Qué Entrega (SubEntregable)</i>	<i>Receptor: Quién recibe o Inspecciona</i>	<i>Criterios: Condiciones de Aceptación</i>	<i>Siguiente paso. Donde va Cuando se Autoriza.</i>
<i>David Córdova</i>	<i>Capitulo Reporte PAP</i>	<i>Profesor PAP (Juan Manuel)</i>	<i>Entregar según el formato establecido en el reporte PAP, y entregar dentro del lapso establecido</i>	<i>ITESO</i>
<i>David Córdova</i>	<i>Reporte de funcionamiento correcto</i>	<i>Profesor empresa (Carlos Eduardo)</i>	<i>Entregar con los requerimientos instalados y funcionando correctamente evidenciando en el reporte</i>	<i>IT Legal Services</i>

2.8 Seguimiento y Control

Tendremos sesiones asignadas con el profesor de la empresa aproximadamente 1 vez cada 2 semanas, en donde compartiremos avances y resolveremos dudas. Lamentablemente sufrimos un retraso al inicio de semestre en donde pudimos empezar con la planeación del PAP hasta 1 mes después del comienzo del semestre, esta es la razón por la que ciertas entregas han estado tardías.

Para la primera entrega debo entregar la investigación de hardware y los protocolos IoT, que usaré el libro de guía para realizar la primera investigación, después nos juntaremos para seleccionar el hardware que vamos a utilizar para comenzar a implementarlo, por lo que mis actividades posteriores serán instalar el sistema operativo al equipo y empezar a realizar la instalación de programas para el escaneo de dispositivos IoT y su respectiva configuración. Después me juntaré con el profesor aproximadamente 2 semanas después para la realización de las primeras pruebas de red en múltiples dispositivos y revisar junto con él que otros campos deberíamos cubrir y exactamente saber cuál es la información que debemos recopilar.

Al mismo tiempo, nuestro profesor PAP nos otorgó un calendario de actividades en donde cada cierto tiempo nos estaremos reuniendo con él para explicación de las entregas del reporte PAP, así como otras sesiones de asesoría ahora que estamos entrando a contextos laborales profesionales.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

Finalmente, trataremos dejar al equipo de IT Legal services un dispositivo en correcto funcionamiento y con distintas funcionalidades que van a ser de utilidad para futuros proyectos, y para que el servicio que ofrece la empresa esté más completo. De mi parte me encargaré de entregar las configuraciones Linux correspondientes y con los programas instalados, así como pre-configuraciones de red y escaneo a dispositivos. Al final sumando las aportaciones y entregables de mis demás compañeros se entregará un dispositivo completo capaz de realizar escaneos a dispositivos IoT

3.2 Estimación del Impacto

Gracias a los dispositivos IoT de escaneo que se traerán del extranjero y configurarán el objetivo es tanto nosotros aprender de dispositivos IoT a también contribuir con este nuevo servicio a la empresa, por lo que de ese lado tendrán una nueva modalidad de escaneo para poder combatir ataques a la red, comportamiento malicioso o dispositivos no reconocidos en dicha red y así mejorar los entregables para que los clientes puedan tener sus sistemas seguros y a futuro la empresa pueda crecer y su mercado de expanda. También para poder dar visibilidad a lo útil que pueden llegar a ser estos dispositivos y pueda yo quedarme con el valioso conocimiento en dado caso que tenga que implementar uno nuevamente en el futuro.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

De momento las competencias más importantes que desarrollé fueron:

- Administración y configuración de sistemas Linux
 - Programación scripting
 - Análisis y seguridad en redes
 - Uso de herramientas open-source
 - Comunicación efectiva en equipos técnicos
- ¿Cuáles fueron las competencias técnicas que desarrollaste propias de tu profesión, así como las genéricas?
Creo que de las técnicas el uso de administración de sistemas Linux fue lo principal, de ahí en más las demás herramientas open-source abarcaron varias disciplinas genéricas y aprender de dichas herramientas para poder escanear dispositivos fue de lo que más aprendí
 - ¿Cuáles fueron las competencias suaves que desarrollaste en tu participación PAP?
Comunicación con colegas de otras disciplinas o áreas y discutir o explicar resultados
 - ¿Cuáles fueron tus aprendizajes más importantes sobre el contexto sociopolítico y económico, y la problemática observada de tu campo profesional?
Que el área de la ciberseguridad no está muy abarcada, hay muchas empresas que lo necesitan y el hecho de que se vayan creando más corporaciones con este fin abre un buen mercado de empleo a estudiantes de este campo y las empresas se benefician al tener seguridad implementada
 - ¿Cuáles fueron los saberes adquiridos en los estudios universitarios que fueron puestos a prueba en tu PAP?
Diseño de aplicaciones y servicios web, administración de redes, de sistemas y el uso de sistemas Linux a través de las últimas materias de gestión de la ciberseguridad
 - ¿Qué tan capaz eres ahora para definir un proyecto (*o parte de él*); con base en objetivos de mejora social; o bien, para hacer su seguimiento y evaluar su puesta en práctica; para tomar decisiones?
Considero que esta experiencia me ayudó mucho al momento de comprender cómo se le vende un servicio a un cliente y poder explicar de manera sencilla el proceso que hacemos y su importancia en el mercado, por lo que si tuviera que implementar un proyecto así (fuera de las inversiones iniciales que podrían ser altas), reconozco que puedo tener los conocimientos para llevarlo a cabo satisfactoriamente.

4.2 Aprendizajes Sociales

- ¿Qué prácticas sociales y en qué ámbitos de la sociedad en los que crees que puedes innovar?
Así como los contadores y abogados son roles vitales en una empresa hoy en día, la seguridad también lo es, mayor parte de la sociedad se comunica a través de dispositivos conectado a la red y, por ende, nuevos peligros surgen con la tecnología, aprender de esto y saber cómo defendernos es un gran aporte para asegurar la confidencialidad de la sociedad.
- ¿A qué grupos sociales benefició el proyecto?
Todo aquel que use un dispositivo conectado a una red
- ¿Mis servicios profesionales produjeron bienes de carácter público?, cuáles?
Otorgaron visibilidad de dispositivos de escaneo no usuales en México
- ¿Mis servicios profesionales ayudan a grupos que no disponen de recursos para generar bienes sociales, en la actualidad o a futuro?
No, quizá para futuro sí.
- ¿Mis servicios profesionales contribuyen para mejorar la economía del país, o región?
No completamente
- ¿Cambiaron mis supuestos y/o visión del mundo social sobre la realidad?
No
- ¿En qué forma pude desplegar una iniciativa de transformación de la realidad, con creatividad, innovación, espíritu emprendedor y orientado a la calidad de la vida social?
Empezar a realizar algo que te gusta y que sepas que tus aportaciones serán valiosas para otras personas, por lo que considero que será más fácil realizar proyectos de este estilo.

4.3 Aprendizajes Éticos

- ¿Encuentras similitud y concordancia entre tus valores personales y el Sentido Social de la Empresa Huésped donde realizaste tu PAP?
Sí, mejorar la calidad de los sistemas para una mejor experiencia al cliente
- ¿Identifico después de esta experiencia vivida, hacia dónde me lleva o invita en mi vida profesional y personal?
Sí, confirmo que es el área profesional a la que me quiero dedicar
- ¿Tuve que tomar decisiones que se dieron bajo que contexto de incertidumbre ética, por qué razón las tomé, y qué consecuencias tuvieron?
No
- ¿Me queda claro, cómo y para quien habré de ejercer mi profesión después de la experiencia del PAP?
Sí

4.4 Aprendizajes Personales

- ¿La experiencia del PAP me dio elementos que ayudan para conocerme mejor, mis habilidades y mis potencialidades?
Sí, me ayudó a confirmar mi gusto por la ciberseguridad
- ¿La experiencia del PAP me da una nueva visión para conocer y reconocer otros aspectos de la sociedad y a las personas?
Sí, me ayudó a conocer cómo se introduce la ciberseguridad a una nueva compañía como servicio y su importancia en la sociedad
- ¿Cómo me ayudó el PAP para aprender a convivir en la pluralidad y para la diversidad?
Me ayudó a saber resolver situaciones de contratiempos, diversos problemas de logística y resolver problemas en equipo
- ¿El haber participado en PAP me ha dado enseñanzas para entender y proyectar mejor mi Proyecto de Vida Personal y Profesional?
Sí, me da un panorama de mayor experiencia en este mercado para poder entender cómo funciona y salir preparado al mundo real laboral

4.5 Tareas Aprendidas

Principalmente me ayudó el hecho de que todos queremos terminar y sacar adelante el trabajo, por lo que con lo que más me quedo es con el compañerismo, comunicación y trabajo en equipo, ya que surgieron distintas situaciones en donde no entendíamos como implementar o juntar una funcionalidad y el hecho de estar trabajando en conjunto y cada quien resolviendo en lo que era bueno, fue de mucha ayuda para la conclusión del proyecto, creo que el hecho de garantizar de que la comunicación es efectiva es vital para un próximo proyecto en el que vaya a participar

Así mismo, la información y material otorgados por el profesor nos sirvió de mucha ayuda a la hora de comprender como funcionan estos dispositivos y toda la implementación, también el hecho de estar en constante supervisión y estar pidiendo ayuda de la manera correcta es de las cosas más importantes de las que me quedo

5. Conclusiones

Me quedo con muchas cosas aprendidas en este proyecto, debido a que es de mis primeras experiencias laborales en el mundo de la tecnología, reconozco que he logrado adquirir nuevas habilidades técnicas y sociales, el hecho de aprender a configurar un pequeño dispositivo Linux me da entendimiento de todo lo que puedo lograr con este sistema operativo y del provecho que puedo sacar a todas esas implementaciones. En general creo que además de aprender de nuevas herramientas y crear nuevas aplicaciones, reforzaron mi conocimiento en este sistema operativo y de redes, las cuales fueron las principales metodologías que desarrollamos durante el proyecto y creo que son vitales para un ingeniero en ciberseguridad, agradezco mucho esa experiencia ya que a las empresas grandes les importa que hayas trabajado en una implementación real, y la que hicimos en este PAP terminó siendo de mucha utilidad.

Asimismo, considero que la comunicación fue el otro parámetro que desarrollé mucho, ya que antes me costaba un poco saber explicarme y más cuando es algo técnico y se tiene que mencionar en inglés para todo el equipo, pero gracias a las juntas seguidas que teníamos y la paciencia de los compañeros pudimos avanzar bien, pude darme a expresar correctamente y me pude adaptar a estas condiciones sociales para que todos podamos avanzar de manera eficaz y sin contratiempos. Si tuviera que cambiar algo (pero al final me doy cuenta de que fue de gran aprendizaje) fue el hecho de tener contratiempos con la comunicación con el líder de la empresa al inicio, sin embargo reconozco que este proceso fue un claro ejemplo para poder saber cómo proceder al momento de un contratiempo o haya algún problema externo a nosotros, cómo comunicar que estamos bloqueados y estar dispuestos a buscar distintas alternativas para no perder tanto el tiempo en lo que se resuelve el problema.

En conclusión, creo que este PAP me deja mucha enseñanza como desarrollo profesional y laboral, tengo entendido cómo relacionarme con equipos de todo el mundo y con clientes con distintas necesidades/exigencias. Y sobre todo logré adquirir conocimiento valioso de ciberseguridad además de la adquirida en la universidad. Espero con ansias poder implementar el PAP 2 para ver qué sorpresas y nuevos retos encontraré.