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: ICS, Emiliano TREJO Rios

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

Tlaquepaque, Jalisco, mayo 2025

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

La identificación y clasificación de dispositivos IoT dentro de una red es una necesidad creciente en el ámbito de la ciberseguridad, dado el incremento de amenazas y la proliferación de dispositivos conectados sin un control adecuado. Este proyecto tiene como objetivo desarrollar un dispositivo de hardware y software capaz de detectar y clasificar dispositivos IoT en una red, identificando posibles intrusos o elementos no autorizados.

A lo largo de este documento expone cuales fueron los hitos que se han desarrollado al largo del proyecto y se aborda la relevancia de contar con herramientas de monitoreo automatizado en entornos donde la cantidad de dispositivos conectados dificulta su administración y control manual.

La elaboración de este proyecto ha sido enriquecida por la experiencia adquirida en el Proyectos de Aplicación Profesional (PAP) previo en el que participé. En estos, tuve la oportunidad de aplicar metodologías de análisis de seguridad, evaluación de infraestructura tecnológica y generación de reportes ejecutivos y técnicos dirigidos a distintos niveles organizacionales. Estas experiencias permitieron estructurar un enfoque sólido para el desarrollo del dispositivo, priorizando la claridad en la presentación de datos y la viabilidad de su implementación en entornos reales.

Los entregables incluyen documentación técnica detallada sobre el funcionamiento del dispositivo, los métodos utilizados para la detección y clasificación de dispositivos IoT, así como un reporte ejecutivo que presenta los hallazgos de manera accesible para tomadores de decisiones. Además, se proponen recomendaciones para fortalecer la seguridad de las redes donde se implemente la solución.

Este proyecto busca no solo ofrecer una herramienta útil para la gestión y protección de redes, sino también contribuir al desarrollo de estrategias más eficaces para la identificación de amenazas en entornos altamente conectados. Con ello, se espera facilitar

la toma de decisiones en materia de seguridad informática y optimizar la respuesta ante posibles vulnerabilidades.

1. Introducción

1.1 Antecedentes

La organización huésped actual es IT Legal Services, un despacho especializado en ciberseguridad combate de delitos tecnológicos y cómputo forense. Su objetivo principal es brindar 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.

Las principales ramas tecnológicas en las que se enfoca incluyen ciberseguridad, gestión de riesgos, cumplimiento normativo en TI y consultoría en transformación digital. Dentro de estas áreas, la empresa desarrolla herramientas para la protección de redes, realiza análisis de vulnerabilidades y implementa soluciones de monitoreo.

La empresa atiende a una amplia gama de clientes, incluyendo PYMES, empresas de manufactura, sector financiero, servicios y organismos gubernamentales. Su presencia y mercado principal abarcan territorios nacionales.

La misión de la organización es proteger a empresas, instituciones y personas del cibercrimen mediante soluciones innovadoras de ciberseguridad, análisis forense digital y consultoría en delitos tecnológicos. El objetivo es garantizar la integridad, confidencialidad y disponibilidad de la información, brindando respuestas efectivas ante incidentes de seguridad y contribuyendo a la justicia digital con investigaciones forenses precisas y éticas.

1.2 Justificación

A lo largo de la carrera siempre me ha interesado todo lo relacionado a las auditorias, el análisis exhaustivo de las políticas de alguna empresa para encontrar áreas de mejora y el cuestionamiento de cuando las políticas impuestas no se están cumpliendo. Ya que este

PAP requiere que desarrollemos un dispositivo capaz de detectar dispositivos IoT no autorizados en una red, me permite ampliar mi conocimiento en esta área, lo cual me permitirá evaluar mejor este tipo de dispositivos en un ámbito profesional cuando me encuentre con ellos en alguna auditoria.

Dado que estoy en mis últimos semestres, puedo dedicar el tiempo necesario para realizar este proyecto de la mejor manera posible, segregando de manera adecuada mis actividades para tener un orden y lograr los objetivos y milestones que se definieron para considerar el proyecto como un éxito.

1.3 Objetivos

Una de las palabras clave de la visión de IT Legal Services es ser referencia en innovación, excelencia y compromiso, por lo cual debemos de brindar una solución en colaboración con la empresa huésped que este a la altura de dicha visión. El entregable principal será un sensor basado en hardware y software que permita el descubrimiento de dispositivos IoT conectados a la red o dentro de un hogar y poder brindar un semáforo de riesgos de explotación, además de toda la documentación necesaria para soportar el proyecto, como su funcionamiento y las pruebas que se realizaron para justificar su producción.

El objetivo que espero conseguir con este PAP es observar cómo es que se trabaja en el mundo real en cuanto a temas de análisis de IoT se refiere, ya que no es algo usual de encontrar, se tiene que realizar un análisis profundo para encontrar la mayor cantidad de incidencias posibles en este tipo de dispositivos usando los conocimientos adquiridos a lo largo de la carrera.

- Considero que tengo los conocimientos técnicos necesarios para realizar un análisis de vulnerabilidades gracias a todo lo que he visto y practicado de la carrera.
- Tengo toda la disposición y apertura de trabajar en conjunto con mis compañeros para lograr alcanzar los objetivos propuestos para el proyecto.

- Me considero una persona resiliente, con la capacidad de encontrar soluciones a problemas que se puedan presentar a lo largo de proyectos en los que me cuente involucrado.

1.4 Contexto

El proyecto consiste en desarrollar un dispositivo capaz de monitorear una red y detectar dispositivos IoT intrusivos o no autorizados mediante el análisis de tráfico, fingerprinting de dispositivos y un sistema de alertas, para de estar manera mitigar un posible riesgo a la red y los cativos que se encuentren dentro de ella. Se busca utilizar esta implementación en las redes de potenciales clientes de la empresa huésped en las que no se destina un presupuesto elevado para este tipo de soluciones tecnológicas, así como para empresas que busquen identificar cualquier potencial riesgo para sus activos.

En mi caso particular, yo estaré encargado del área de Desarrollo de Backend y API. Mi función será la implementación del servidor backend, desarrollo del API REST para procesar los datos y la gestión de la base de datos.

1.5 Entregables

Los entregables del proyecto serán:

- 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.

1.6 Involucrados

Además de los alumnos que estaremos trabajando en el equipo, nuestro líder técnico junto con otros empleados de IT Legal Services estarán colaborando como facilitadores de algunas herramientas que harán posible los avances necesarios para nuestros entregables.

2. Desarrollo del Proyecto PAP
2.1 Administración del Proyecto

Inicio

Se asignan los roles de los alumnos para el proyecto, así como las tareas asociadas con dicho rol. Se realizan investigaciones de términos y metodologías para comprender mejor el entorno con el que estaremos trabajando.

Planificación

Se divide por semana las fases para cada rol, de esta manera se evita que se crucen momentos clave, por ejemplo, que el Backend no se pueda terminar porque el Frontend todavía está en desarrollo. Se definen los objetivos de cada actividad para no salir del alcance de lo que el dispositivo requiere en primera instancia.

Ejecución

Se usan herramientas tales como Kali, Java y otras utilidades en conjunto con técnicas de desarrollo y análisis para desarrollar el dispositivo, y posteriormente probarlo en una red, escanearla y encontrar dispositivos IoT conectados.

Seguimiento

Cada semana hay dos reuniones agendadas con el líder técnico para reportar de forma periódica nuestros avances y dudas. El líder técnico da retroalimentación y posibles planes de acción en función de lo anterior, o en su defecto, nos prepara para la siguiente fase del proyecto.

Control

El líder técnico establece una lista de resultados esperados de cada fase de los análisis, así como las partes esenciales de los entregables, si durante la fase de seguimiento nota alguna deficiencia o punto importante sobre el que valga la pena elaborar, lo hace saber al equipo.

Cierre

El proyecto se concluye cuando el equipo entrega el dispositivo, así como toda la documentación asociada que cumplan con los requisitos mínimos a los responsables dentro de la empresa huésped.

2.2 Sustento Teórico y Metodológico

El proyecto se maneja de manera iterativa similar a una metodología ágil. Hay una lista de tareas generales a realizar desde el inicio del proyecto separadas por semanas, y dos veces a la semana el equipo tiene reuniones con el líder técnico donde se discute el progreso del equipo con las tareas de la semana y se retroalimenta en caso de ser necesario sobre posibles actividades para complementar las tareas ya establecidas. Dada la dependencia de algunas tareas sobre otras, es importante asegurar que se completan en orden de manera efectiva.

2.3 Descripción del Proyecto

El desarrollo del dispositivo de detección y clasificación de dispositivos IoT en una red sigue una metodología estructurada en diversas fases, asegurando una integración progresiva de los sub-entregables hasta obtener el producto final.

La primera fase del proyecto es la implementación del hardware. En esta etapa, se selecciona y configura el dispositivo físico que servirá como base del sistema de monitoreo. Se instalan herramientas esenciales de análisis de tráfico y detección de dispositivos, además de establecer la comunicación con los sistemas de almacenamiento y procesamiento de datos.

La segunda fase es el desarrollo del backend, donde se implementan los algoritmos de análisis de red y clasificación de dispositivos IoT. Esto incluye la configuración de

herramientas de escaneo pasivo y activo, el análisis de patrones de tráfico, y la integración de bases de datos que almacenen la información recopilada. Durante esta etapa, se establecen protocolos de seguridad y mecanismos de actualización para garantizar un funcionamiento estable y confiable.

La tercera fase consiste en la creación del frontend, una interfaz gráfica que permitirá a los usuarios visualizar los dispositivos detectados, su clasificación y posibles alertas en caso de encontrar elementos no autorizados en la red. Se diseña una plataforma intuitiva con acceso a reportes y métricas clave sobre la actividad en la red.

Finalmente, se realiza la fase de pruebas y validación, en la que se evalúa el desempeño del dispositivo en distintos entornos de red, asegurando su precisión y eficiencia en la detección de dispositivos IoT. Se ajustan los algoritmos según los resultados obtenidos y se documentan los hallazgos en reportes técnicos y ejecutivos.

Para el alcance de este PAP, se espera entregar un prototipo funcional capaz de escanear la red en búsqueda de dispositivos IoT, clasificarlos y generar reportes accesibles mediante la interfaz gráfica.

Durante el desarrollo de este proyecto se utilizan los siguientes recursos clave:

- Herramientas de análisis de red, como software de escaneo pasivo y activo para identificar dispositivos conectados.
- Frameworks de desarrollo, incluyendo entornos para backend y frontend, que faciliten la integración y visualización de los datos obtenidos.
- Plataformas de bases de datos y almacenamiento, para registrar información relevante sobre los dispositivos detectados.
- Sistemas operativos optimizados para seguridad y análisis de tráfico, como distribuciones Linux enfocadas en ciberseguridad.

2.4 Tipo de Proyecto

El proyecto se puede ejecutar bien en cascada si se han definido con claridad los objetivos de las pruebas de penetración, si se ha definido una metodología clara y sólida, pero en nuestro caso se lleva de forma un poco más iterativa dado que las reuniones con nuestro líder técnico funcionan como scrums y cada semana funciona como un sprint. Si bien el desarrollo y las pruebas pueden ser cualquiera de las dos metodologías mencionadas, idealmente solo es una parte en el ciclo de vida de mejora continuo del proyecto.

2.5 Plan de Trabajo

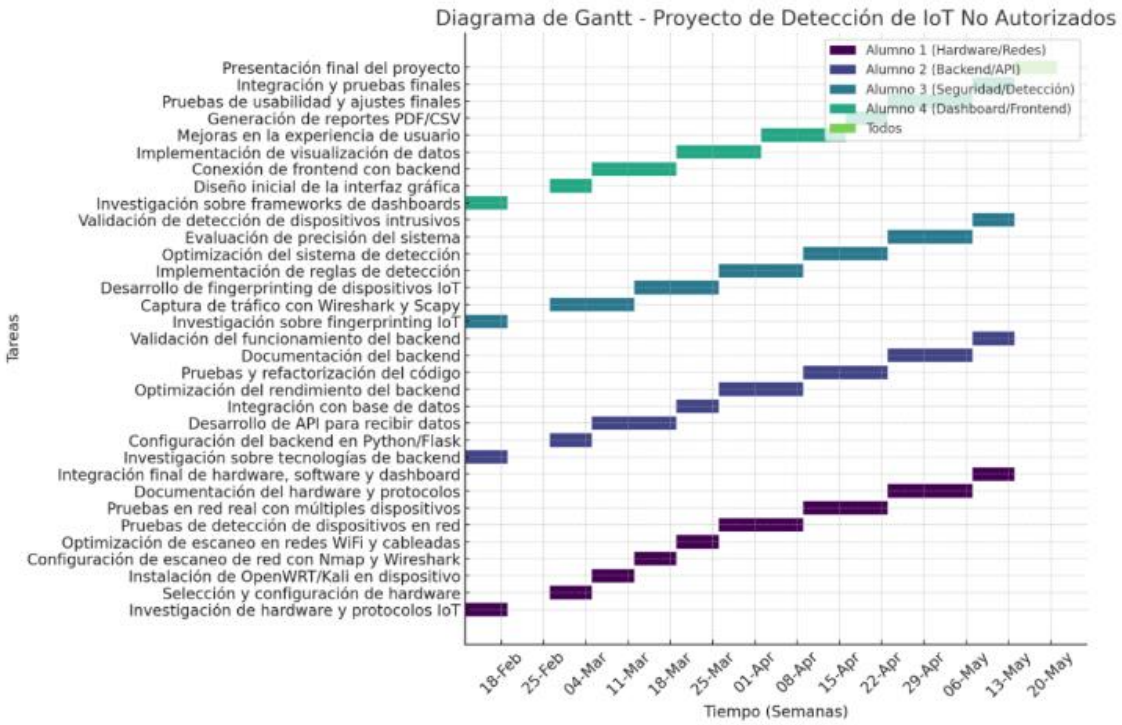
No.	Competencia	Nivel Adquirido al Inicio	Nivel Objetivo al final PAP	Objetivo final PAP	Prior
1	Conocimientos sobre IoT	1	2	2	A
2	Programación Java y Python	1	3	3	A
3	Uso de herramientas de análisis (Kali Linux, Zeek, Suricata, Wireshark, Nmap, Shodan API)	2	2	2	A
4	Conocimiento sobre dispositivos programables (Raspberry PI, ESP32)	1	2	2	A
5	Conocimiento de Bases de Datos (SQLite, MongoDB)	1	2	2	A
6	Dashboards en Web (Flask, FastAPI)	0	2	2	M
7	Desarrollo de Informe técnico	2	2	2	M
8	Presentación de Resultados	1	2	2	M

Plan de trabajo Individual de 14 semanas – 16 horas por semana por alumno.

Semana	Tarea	Responsable	Duración (Semanas)
1 - 2	Investigación de hardware y protocolos IoT	David (Hardware/Redes)	1
3 - 4	Selección y configuración de hardware	David (Hardware/Redes)	1
4 - 5	Instalación de OpenWRT/Kali en dispositivo	David (Hardware/Redes)	1
5 - 6	Configuración de escaneo de red con Nmap y Wireshark	David (Hardware/Redes)	1
6 - 7	Optimización de escaneo en redes WiFi y cableadas	David (Hardware/Redes)	1
7 - 9	Pruebas de detección de dispositivos en red	David (Hardware/Redes)	2
9 - 11	Pruebas en red real con múltiples dispositivos	David (Hardware/Redes)	2
11 - 13	Documentación del hardware y protocolos	David (Hardware/Redes)	2
13 - 14	Integración final de hardware, software y dashboard	David (Hardware/Redes)	1
1 - 2	Investigación sobre tecnologías de backend	Emiliano (Backend/API)	1
3 - 4	Configuración del backend en Python/Flask	Emiliano (Backend/API)	1
4 - 6	Desarrollo de API para recibir datos	Emiliano (Backend/API)	2
6 - 7	Integración con base de datos	Emiliano (Backend/API)	1
7 - 9	Optimización del rendimiento del backend	Emiliano (Backend/API)	2
9 - 11	Pruebas y refactorización del código	Emiliano (Backend/API)	2

Plan de trabajo Individual de 14 semanas – 16 horas por semana por alumno.

11 - 13	**Documentación del backend**	**Emiliano (Backend/API)**	**2**
13 - 14	**Validación del funcionamiento del backend**	**Emiliano (Backend/API)**	**1**
1 - 2	Investigación sobre fingerprinting IoT	Marlem Vela(Seguridad/Detección)	1
3 - 5	Captura de tráfico con Wireshark y Scapy	Marlem Vela(Seguridad/Detección)	2
5 - 7	Desarrollo de fingerprinting de dispositivos IoT	Marlem (Seguridad/Detección)	2
7 - 9	Implementación de reglas de detección	Marlem (Seguridad/Detección)	2
9 - 11	Optimización del sistema de detección	Marlem (Seguridad/Detección)	2
11 - 13	Evaluación de precisión del sistema	Marlem (Seguridad/Detección)	2
13 - 14	Validación de detección de dispositivos intrusivos	Marlem (Seguridad/Detección)	1
1 - 2	**Investigación sobre frameworks de dashboards**	**Federico (Dashboard/Frontend)**	**1**
3 - 4	**Diseño inicial de la interfaz gráfica**	**Federico (Dashboard/Frontend)**	**1**
4 - 6	**Conexión de frontend con backend**	**Federico (Dashboard/Frontend)**	**2**
6 - 8	**Implementación de visualización de datos**	**Federico (Dashboard/Frontend)**	**2**
8 - 10	**Mejoras en la experiencia de usuario**	**Federico (Dashboard/Frontend)**	**2**
10 - 11	**Generación de reportes PDF/CSV**	**Federico (Dashboard/Frontend)**	**1**
11 - 13	**Pruebas de usabilidad y ajustes finales**	**Federico (Dashboard/Frontend)**	**2**
13 - 14	**Integración y pruebas finales**	**Federico (Dashboard/Frontend)**	**1**
14 - 15	**Presentación final del proyecto**	**Todos**	**1**



2.6 Equipo de Trabajo

Rol	*Responsabilidad*	*Nombre (opcional)*
Ingeniero de Hardware y Redes	*Configuración de hardware, instalación de sistemas operativos y configuración de redes para el escaneo de dispositivos.*	*David Córdova*
Desarrollador Backend y API	*Implementación del servidor backend, desarrollo de API REST para procesar datos y gestionar la base de datos.*	*Emiliano Trejo*
Especialista en Seguridad y Detección	*Implementación de Sniffing de tráfico, fingerprinting de dispositivos IoT y detección de amenazas.*	*Marlem Vela*
Desarrollador Frontend y Dashboard	*Diseño e implementación de una interfaz grafica para visualizar y reportar dispositivos detectados.*	*Federico Garibay*

2.7 Plan de Comunicaciones

Emisor	*Mensaje*	*Receptor*	*Medio*	*Frecuencia*
Ingeniero de Hardware y Redes	*Información, reportes*	*Miembros del equipo, líder técnico*	*Microsoft Teams*	*Semanal*
Desarrollador Backend y API	*Información, reportes*	*Miembros del equipo, líder técnico*	*Microsoft Teams*	*Semanal*

Especialista en Seguridad y Detección	*Información, reportes*	*Miembros del equipo, líder técnico*	*Microsoft Teams*	*Semanal*
Desarrollador Frontend y Dashboard	*Información, reportes*	*Miembros del equipo, líder técnico*	*Microsoft Teams*	*Semanal*
Líder Técnico	*Información, plan de trabajo por fase, retroalimentación*	*Miembros del equipo*	*Microsoft Teams & videoconferencias de seguimiento*	*Cada 3 días*

2.8 Plan de Calidad

Emisor: Quién Entrega	*Entregable: Qué Entrega (Entregable)*	*Receptor: Quién recibe o Inspecciona*	*Criterios: Condiciones de Aceptación*	*Siguiente paso. Cuando se Autoriza.*
Desarrollador Backend y API	*Documentación de Backend*	*Líder Técnico*	*Se explica a detalle como es que el backend se desarrollo y como converge con las otras aplicaciones del proyecto.*	*Corregir en caso de ser necesario; preparar para la presentación*
Especialista en Seguridad y Detección	*Reporte de detección de IoTs*	*Líder Técnico*	*Se explica a detalle que vulnerabilidades se encontraron y como estas se reportaron y mostraron en el dispositivo.*	*Corregir en caso de ser necesario; preparar para la presentación*
Desarrollador Frontend y Dashboard	*Documentación del Dashboard*	*Líder Técnico*	*Se explica a detalle cómo se desarrolló el dashboard, así como la manera en la que esta muestra los datos arrojados por las otras aplicaciones del proyecto.*	*Corregir en caso de ser necesario; preparar para la presentación*
Miembros del equipo	*Dispositivo Funcional*	*Líder Técnico*	*Se entrega el dispositivo funcional con todos los criterios mínimos establecidos al inicio del proyecto.*	*Realizar pruebas preliminares; preparar para la presentación*

2.9 Seguimiento y Control

Se estarán realizando juntas semanales con el equipo y líder técnico para revisar el continuo avance del proyecto, dudas referentes a algunos de los hitos por alcanzar y que el plan de trabajo se mantenga en curso.

Con el tipo de metodología Ágil, podemos garantizar que, de ser necesario, se podrían realizar cambios en alguno de los puntos clave del proyecto, ya sea actualizar el enfoque

para el desarrollo del backend y dashboard, o para la implementación de herramientas de análisis nuevas para el dispositivo.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

- Código fuente documentado del Backend, dashboard y detección de IoTs.
- Informe técnico detallado con la descripción de la arquitectura, metodologías y resultados.
- Dispositivo para detectar IoTs en una red funcional.

.

3.2 Estimación del Impacto

Uno de los principales resultados es el código fuente documentado del backend, el dashboard y el sistema de detección de dispositivos IoT. Este código proporciona la base para futuras mejoras y optimizaciones, facilitando la escalabilidad y el mantenimiento del sistema. Además, se elaboró un informe técnico detallado que describe la arquitectura del sistema, las metodologías utilizadas y los resultados obtenidos. Este documento es clave para comprender el funcionamiento del dispositivo desarrollado y brinda información útil para su implementación y mejora desde un enfoque más específico y hecho para gente con conocimientos más especializados. Por último, se entregó un dispositivo funcional para la detección de dispositivos IoT en una red. Este hardware permite escanear y clasificar dispositivos conectados, proporcionando información valiosa sobre posibles elementos no autorizados y facilitando su monitoreo en tiempo real.

Estos entregables permiten a la empresa huésped tener una base sólida para utilizar el dispositivo en los clientes que soliciten dicho servicio, proporcionando herramientas concretas para la detección y mitigación de amenazas relacionadas con dispositivos IoT.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

- ¿Cuáles fueron las competencias técnicas más significativas que desarrollaste propias de tu desarrollo profesional?
  - **Utilización de Herramientas de Análisis de Seguridad:** Genere experiencia práctica con herramientas como Nmap, Suricata y Wireshark, entre otras. Estas herramientas fueron fundamentales para la identificación y análisis de vulnerabilidades.
  - **Gestión de Herramientas de Programación:** Desarrollamos el uso de herramientas de programación como Python y Java para el desarrollo del Backend y otros aspectos clave del software del dispositivo.
  - **Utilización de Herramientas para gestión de Bases de Datos:** Generamos experiencia con la utilización de bases de datos como MongoDB en un entorno mas real para la gestión de la información que obtuvimos del dispositivo para poder almacenarla.

- ¿Cuáles fueron las competencias llamadas suaves o emocionales que mayormente impactan y creciste para tu desarrollo personal y profesional en tu participación PAP?
  - **Trabajo en Equipo:** Colaborar con un equipo multidisciplinario fue fundamental para el éxito del proyecto. Aprendí a valorar y aprovechar las distintas habilidades y conocimientos de mis compañeros, fomentando un ambiente de colaboración y apoyo mutuo. Esto mejoró mi capacidad para trabajar en equipo y fortalecer relaciones profesionales.
  - **Solución de Problemas:** Enfrentar y superar desafíos técnicos y organizacionales durante el proyecto me permitió desarrollar habilidades avanzadas de solución de problemas. Aprendí a abordar problemas complejos de manera estructurada, identificar las causas raíz y proponer soluciones efectivas.
  - **Adaptabilidad:** La naturaleza dinámica del proyecto requirió una gran flexibilidad y capacidad para adaptarme a los cambios imprevistos. Ajustamos los planes y estrategias según fuera necesario para los requerimientos que fueran presentándose en el proyecto.

- ¿Hubo sorpresas importantes sobre el contexto sociopolítico y económico y la problemática de tu campo profesional que hayas descubierto?

  En cuanto al tema de seguridad, detectar y clasificar dispositivos IoT en una red no es una tarea sencilla, ya que muchos de ellos no responden a escaneos tradicionales y pueden utilizar direcciones IP dinámicas o mecanismos de comunicación no convencionales. La falta de estándares de identificación dificulta su monitoreo efectivo y por lo tanto pudimos identificar un área compleja al trabajar con estos dispositivos.

  A su vez, también me di cuenta de que las consecuencias económicas de las brechas de seguridad pueden ser devastadoras para las organizaciones. Una sola vulnerabilidad explotada puede resultar en pérdidas económicas sustanciales, tanto por daños directos como por la pérdida de confianza de los clientes. Esta realidad subraya la importancia de invertir en medidas de seguridad adecuadas.

  Como último punto del cual me pude percatar, es que las organizaciones suelen carecer de una conciencia adecuada sobre la importancia de la ciberseguridad. A menudo, la ciberseguridad no es una prioridad para estas empresas hasta que sufren un incidente significativo. Este descubrimiento resalta la necesidad de campañas de concientización y educación en ciberseguridad para todas las organizaciones, independientemente de su tamaño.

- ¿Cuáles fueron los saberes que debiste haber adquirido en tus estudios universitarios que Fueron puestos a prueba en el PAP y no los tenías?

  Particularmente no tuve saberes que debí haber aprendido y no lo hice. Todas las herramientas y metodologías que utilizamos las había visto con anterioridad en mi carrera universitaria, solamente no las había aplicado en un contexto profesional, pero con la ayuda y asesoramiento de nuestro líder técnico, logramos dirigir y focalizar esos saberes a un ámbito profesional para poder realizar nuestras pruebas sin mayores complicaciones. En su mayor parte, fue ponernos a prueba en cuanto a conocimientos de las herramientas que previamente habíamos utilizado.

- ¿Te consideras ahora que eres capaz ahora para preparar un proyecto (*o parte de él)*; como para dirigirlo, o con un poco más de preparación serás suficientemente capaz en un futuro próximo con base en objetivos, a la mejora social; para hacer su seguimiento y evaluar su puesta en práctica; para tomar decisiones?

  Considero que ahora soy más capaz de preparar un proyecto o parte de él, y con un poco más de preparación, seré suficientemente capaz en un futuro próximo para dirigirlo completamente.

  A través de mi participación en el desarrollo de este dispositivo para la detección de IoTs, he desarrollado una base sólida en la planificación y ejecución de proyectos técnicos. Este proceso me ha permitido comprender mejor los componentes esenciales de la gestión de proyectos, incluyendo la definición de objetivos claros, la asignación de recursos, y el seguimiento del progreso.

  Sin embargo, reconozco que aún hay áreas en las que necesito más preparación para ser completamente competentes en la dirección de proyectos complejos. Estas áreas incluyen la gestión de equipos multidisciplinarios, la toma de decisiones estratégicas bajo presión, y la evaluación continua del impacto social y económico del proyecto.

  Dicho lo anterior, estoy comprometido a continuar con mi desarrollo profesional a través de la formación adicional y la práctica en proyectos reales. Con este enfoque, confió en que pronto alcanzare un nivel de competencia que me permitirá no solo preparar y dirigir proyectos, sino también asegurar su éxito y contribuir de manera significativa a la mejora social y organizacional.

4.2 Aprendizajes Sociales

- ¿A qué grupos sociales benefició el proyecto?
  - Empleados de IT Legal Services: El objetivo del proyecto constituye proporcionar herramientas (en este caso los reportes y el dispositivo) que ayudan a la empresa a brindar un mejor servicio a sus clientes.
  - Socios de IT Legal Services: El que la compañía se interese por la seguridad y trabaje activamente en crear innovaciones en sus servicios, puede mejorar su relación de confianza con sus socios comerciales y proveedores.

- Clientes de IT Legal Services: Se obtiene el beneficio de una empresa que opera con normalidad y con menores riesgos de ver comprometidos los datos de sus clientes.

- ¿Tus servicios profesionales contribuyen en algo para mejorar la economía del país, o región?

  Es importante para la continuidad de negocio de las organizaciones tener infraestructuras lo suficientemente protegidas de ciber amenazas; por ejemplo, en Europa se estima que 6 de cada 10 PyMEs cierran 6 meses después de un ciberataque, especialmente si se trata de secuestros informáticos y de datos [2]. Dado que el panorama de la ciberseguridad es de naturaleza cambiante, es importante que las compañías no ignoren esta dimensión de sus activos tecnológicos si quieren tener un desarrollo sano.

  Por lo tanto, este nuevo servicio que podrá brindar IT Legal Services ayuda en gran medida a mitigar un tipo de ataque a dispositivos los cuales no tienden a ser tomados muy en cuenta en las organizaciones, previniendo así el fallo en las operaciones de muchas empresas, sean chicas, medianas o grandes.

- ¿Cambiaron tus supuestos y/o visión del mundo social sobre la realidad?

  Para mí cambio la manera en la que veo las buenas prácticas de seguridad específicamente en dispositivos IoT. Al ser un sector en constante crecimiento, se deben de prever y generar estrategias para la correcta mitigación y contención de riesgos que podrían afectar la operatividad de estos dispositivos. Al ser algo bastante nuevo todavía, se está a tiempo de implementar las medidas necesarias para mantener la seguridad de ellos antes de que se vuelve algo demasiado grande y sea más complicado implementar medidas de mitigación desde cero.

- ¿En qué forma pudiste desplegar una iniciativa de transformación de la realidad, con creatividad, innovación, espíritu emprendedor y orientado a la calidad de la vida social?

  El objetivo del proyecto es innovador, llama mucho a investigar sobre las nuevas tecnologías que empiezan a emerger, para compilar la información relevante necesaria

para el desarrollo de este tipo de medidas de prevención, que serían parte de un plan de mejora para una empresa, y de esta manera seguir siendo confiable para sus clientes y socios.

4.3 Aprendizajes Éticos

- ¿Encuentras similitud o concordancia entre tus valores morales personales y el Sentido Social de la Empresa Huésped donde realizas tu PAP?

  IT Legal tiene una visión que va muy de acuerdo con mis valores morales y también sociales. Son una empresa que no solo se centra en las grandes empresas, sino también en las pequeñas, ser accesibles con sus servicios para poder brindar la protección y asesoramientos adecuados a esas empresas que más lo podrían necesitar. No se trata de ayudar solamente a los más grandes, ya que ellos generalmente tienen más experiencia en los campos de seguridad, las pequeñas y medianas empresas son las que suelen carecer de un contexto acerca de temas de ciberseguridad y por ende son más propensas a caer en un ciberataque. Si podemos brindar el apoyo necesario para que puedan mantener su seguridad y así seguir creciendo, habremos impulsado no solo a la empresa huésped, sino también a sus clientes.

- ¿Qué dilemas morales identificas que se te han presentado, o se podrían presentar a lo largo de tu experiencia PAP? Descríbelos.

  La organización cliente finalmente tiene la última palabra sobre qué hacer respecto a las vulnerabilidades encontradas, es parte de los reportes calificar el valor de un riesgo y adjuntar las sugerencias necesarias para corregir las vulnerabilidades, pero para lo que nosotros podamos considerar algo importante o crítico, puede que la empresa lo considere parte de su flujo de trabajo y decida aceptar el riesgo. Si bien no seremos parte de la toma de decisiones que vengan después de la presentación de los reportes, es importante encontrar este balance entre hacer las sugerencias justas a cada vulnerabilidad sin sesgarlas.

- Frente a lo vivido en tu experiencia PAP, qué implicaciones éticas encuentras que se podrían dar en el ejercicio de tu profesión.

  Durante el ejercicio de mi profesión es probable que me vea en situaciones donde si puede que tenga la posibilidad de intervenir en las decisiones sobre la respuesta a riesgos, y es importante considerar que los recursos de cualquier compañía son finitos, por lo que es necesario priorizar algunas soluciones sobre otras y tratar de que sean sensibles al contexto de la organización. Es común que para los directivos el área de TI sea un gasto antes que cualquier otra cosa, por lo que no hay mucha predisposición a invertir en ella; es entonces mi responsabilidad como profesionista en ciberseguridad promover la iniciativa.

4.4 Aprendizajes Personales

- ¿En qué aspectos de tu vida personal identificas que has cambiado en la forma en que te relacionas con tu familia, tus amigos, compañeros, y en general con la gente que convives?

  Me ha ayudado a valorar aún más el trabajo que cada uno ejerce. Cada persona tiene sus propias áreas de especialidad, y con esta experiencia yo pude conocer las mías, y con esto valoro más las que mis conocidos también tienen. No es fácil vivir con la presión de hacer las cosas bien en el ámbito profesional y ahora soy más consciente de esto con el proyecto que realizamos. Ha cambiado también mi forma de expresarme de mí, me siento orgulloso de los conocimientos y de las metas que he alcanzado en mi vida, y me siento más que preparado para seguir alcanzando nuevas.

- ¿Esta experiencia te ha dado mayor seguridad en tus ideas, propósitos, y manera de reaccionar y actuar en el aspecto personal y/o profesional?

  Esta experiencia definitivamente me ha dado mayor seguridad en mis interés y propósitos, me dio ese empujón adicional para seguir mejorando en mis conocimientos y competencias técnicas. Me ha dado la seguridad para decir “soy capaz, y puedo hacerlo”, algo de lo que siempre dude antes de conseguir un empleo formal en un área de mi carrera, ahora con esta nueva experiencia cada vez me siento más seguro de que puedo hacer las cosas y que si me empeño en ello, puedo conseguirlo.

- ¿Consideras que la experiencia del PAP te dio madurez en diferentes aspectos de tu vida personal?

  Esta experiencia también me brindo madurez a nivel profesional, una probada de cómo es que funciona el mundo laboral y que es lo que se puede esperar de uno en ámbitos profesionales. Me dio también la madurez para entender que eventualmente esto es lo que terminare haciendo para vivir, un golpe de realidad que siento que todos necesitamos recibir en algún momento.

- ¿La experiencia del PAP te dio elementos que ayudan para conocerte mejor, reconocer tus habilidades y tus potencialidades?

  Con la experiencia adquirida en el PAP, puedo decir que conozco mejor mis habilidades y cuáles son las que necesitan mejorar, que es lo que más me apasiona de mi carrera y que no tanto, en qué tipo de actividades soy más eficiente y en cuáles no. En resumen, me dio la capacidad de decidir a qué área me gustaría enfocarme del alto espectro de posibilidades que brinda nuestra carrera universitaria.

- ¿Consideras que la experiencia PAP te ayudo para aprender a convivir en la pluralidad y para la diversidad?

  Por último, esta experiencia me ayudo a convivir y relacionarme con mis compañeros de trabajo, y buscar la sana convivencia para poder realizar nuestras actividades de la mejor manera posible, y brindar un sentimiento de apoyo para aquellos que tal vez tengan dudas acerca de su capacidad para hacer el trabajo.

4.5 Tareas Aprendidas

a.- Cuáles son los factores, las acciones y/o las actitudes que influyeron favorablemente para que se dieran los resultados exitosos del proyecto (tuyas, líder, equipo). El propósito de numerarlas es que los reconozcas y documentes lo que deben debes repetir en ocasiones futuras en tu desempeño profesional y personal.

El haber mantenido una comunicación abierta por parte de todos los miembros del equipo, tanto del equipo como de nuestro líder técnico fue crucial para alinear los esfuerzos y resolver los problemas que fueron presentándose a lo largo del proyecto. Esta claridad en

la comunicación ayudo a evitar cualquier tipo de malentendido y garantizo que todos estuviéramos en la misma página.

A su vez, también fue crucial la colaboración y apoyo mutuo dentro del equipo, esto ayudo a abordar los desafíos técnicos y completar las tareas designadas que se tenían definidas. La disposición de cada miembro del proyecto a aportar con sus conocimientos y habilidades impacto de manera positiva para el éxito del proyecto.

El mantener una documentación detallada de los resultados que íbamos adquiriendo de nuestras evaluaciones ayudo a crear un registro claro y preciso del trabajo realizado, con lo cual pudimos realizar un informe técnico final organizado y preciso para cubrir los puntos clave que desarrollamos en el proyecto.

Con todo esto, podemos dar un indicio para futuros proyectos en los que nos involucremos, para así no solo brindar un buen servicio, sino mejorar nuestras capacidades para seguir desarrollándolas en un entorno laboral.

b.- Cuales fueron las situaciones, las acciones y/o las actitudes que pudieron realizarse de una mejor manera, y que influyeron de manera importante para que los resultados del proyecto no se dieran con la calidad, la oportunidad, a los costos previstos (tuyas, líder, equipo). Esta revisión te servirá para no te pase desapercibido y tengas cuidado en ocasiones y proyectos futuros.

Aunque contaba con los conocimientos técnicos, hubo momentos en que una formación técnica más avanzada hubiera sido beneficiosa, ya que me hubiera dado herramientas más avanzadas para poder implementar en el dispositivo, y así podría haber conseguido que se arrojaran datos más exhaustivos que no entraba en el alcance, pero que no hubiera estado de más o hubieran agilizado el proceso de análisis y descubrimiento.

4.6 Desarrollo Profesional

Las tareas tecnológicas en las que más me interesa desarrollarme, junto con los tipos de proyectos que me gustaría trabajar son:

1. Proyectos que involucren tareas relacionadas con la auditoría de sistemas de información.

2. Tareas y proyectos relacionados con la consultoría para certificaciones como la ISO27001.
3. Tareas y proyectos relacionados con la realización de controles GITC basados en estándares de la industria como la NIST.

Continuando con las áreas en la que me desenvuelvo con mayo destreza:

1. Gestion de riesgos para la seguridad de la información.
2. Administración de arquitecturas de red y servicios que corren dentro de la misma.
3. Auditoria para procedimientos y controles básicos presentes en las políticas de distintas compañías.

Las areas de mayor crecimiento y desarrollo basándonos en mis áreas de interés y habilidades son:

1. Servicios de auditoría y consultoría de procedimientos y políticas para seguridad de la información para terceros.
2. Consultoría para certificaciones como la ISO27001 a empresas.
3. Áreas de administración y gestión de redes.

Para poder alcanzar mis objetivos profesionales en estas áreas debo de considerar especializarme con certificaciones para esos puestos como un CISM (Certified Information Security Manager) [1] o un CCNA (Cisco Certified Network Associate) [3], de esta manera no solo reforzare mis conocimientos y habilidades dentro de estas áreas, sino que tendré un documento que beneficie mis etapas de reclutamiento, avalando que en efecto cuento con los conocimientos que digo tener. Esto mi ayudara a estar un paso más cerca de conseguir cualquiera de estas posiciones. También debo considerar mucho el autoaprendizaje, la realización de cursos para relacionados a mis áreas de interés también puede brindarme la otra posibilidad de demostrar mis habilidades además de expandirlas.

Debido a la creciente curva de ciberataques que las empresas han estado sufriendo en los últimos años, el mercado de la auditoria a sistemas de información también ha visto un incremento de bastante importancia. Las compañías quieren mantener sus activos seguros a toda costa, y siempre se estará buscando gente que pueda ayudarles a validar que sus sistemas se encuentran los suficientemente blindados para evitar alguna amenaza, por lo cual la tendencia por la ciberseguridad y auditoria de la misma está en su punto más alto hoy en día.

Actualmente ya tengo varios proyectos en los que estoy trabajando con una empresa de auditoría, con diversas empresas que buscan la auditoria de sus políticas para la seguridad de la información. Ahí es donde planeo enfocar mis esfuerzos para desarrollarme profesionalmente debido a la gran cantidad de cosas que puedo y he aprendido, además de que ya estoy muy familiarizado con cómo funcionan este tipo de proyectos.

5. Conclusiones

La experiencia en este PAP me ha dejado varias enseñanzas significativas, como lo es la importancia de tener un acercamiento con el mundo real, el ver como todo lo que he estado aprendiendo en la carrera, puede servir ya aplicado a un entorno real, y más importante, el poder poner en práctica mis conocimientos.

Durante mi participación en el PAP, surgieron varias situaciones imprevistas que también me dejaron otro tipo de enseñanzas valiosas. Entre ellas, la importancia de mantener una comunicación efectiva con mis compañeros, quien, como yo, fueron una parte fundamental para que lográramos consolidar el proyecto, también el mantener contacto estrecho con nuestro líder técnico ayudo a que consiguiéramos alcanzar los objetivos establecidos al inicio del proyecto. Esta experiencia me ha enseñado la importancia de la adaptabilidad y la colaboración en equipo, competencias que seguramente me acompañarán en mi futuro desarrollo personal y profesional.

Una de las mayores lecciones aprendidas para mí fue la gestión de las herramientas que utilizamos, esto me proporcionó una comprensión más profunda de cómo reunir y analizar información relevante en un entorno real para identificar posibles vulnerabilidades en sistemas y redes. Esta competencia, junto con el análisis de riesgos, la gestión de proyectos y la coordinación de equipos, son habilidades técnicas que han fortalecido mi perfil profesional. Hubo también descubrimientos importantes relacionados con el contexto sociopolítico y económico que afectaron nuestro campo profesional. La creciente preocupación por la ciberseguridad a nivel global y la necesidad urgente de proteger la información crítica de las empresas fueron revelaciones que subrayaron la relevancia de nuestro trabajo y la demanda de profesionales capacitados en esta área.

A pesar de los logros alcanzados, reconozco que aún necesito más preparación para poder dirigir proyectos de manera autónoma en el futuro. Sin embargo, con el conocimiento y la experiencia adquiridos durante este proyecto, me siento más preparado para asumir roles

de mayor responsabilidad y contribuir a la mejora social a través de la implementación y seguimiento de iniciativas de ciberseguridad.

Al término de esta etapa, siento un alto grado de satisfacción personal. El reto que representó este proyecto, junto con el esfuerzo requerido para lograr mis objetivos, se tradujo en resultados positivos que pude ver reflejado en los entregables que realizamos. La oportunidad de aplicar conocimientos teóricos en un entorno práctico, enfrentar desafíos reales y aprender de cada experiencia ha sido bastante enriquecedor.

Considero que debo mejorar más mi parte para documentar y generar reportes, ya que fue un tema que pude haber hecho mejor, pero tomo esta experiencia como un aprendizaje para hacerlo, ya que había tenido muy poca experiencia haciéndolo en un ámbito profesional.

6. Bibliografía y Anexos

[1] ISACA (2025). Certified Information Security Manager [Online]. Disponible en: https://www.isaca.org/credentialing/cism

[2] Gonzales R. & CincoDías (2023, 12 de junio). Seis de cada diez pymes en Europa acaban cerrando cuando sufre un ciberataque [Online]. Disponible en: https://cincodias.elpais.com/cincodias/2023/06/06/pyme/1686074080_605400.html

[3] CISCO (2025, 14 de Febrero). CCNA Certification [Online]. Disponible en: https://www.cisco.com/site/us/en/learn/trainingcertifications/certifications/enterprise/ccna/index.html