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 GESTION E INNOVACION EN INGENIERIA DE PRODUCTO

BIDAIDEA

PRESENTA

Alumno: ISI LEÓN GUILLERMO GARCÍA CERPA

Profesor PAP: Juan Manuel Islas Espinoza, PMP®

Tlaquepaque, Jalisco, diciembre de 2022.

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

Mi proyecto PAP se trata del descubrimiento y tratamiento de vulnerabilidades en la infraestructura de varios clientes, en el cual se nos pide hacer investigaciones en los servicios de los clientes para posteriormente realizar un reporte de análisis de vulnerabilidades para llevar a cabo las medidas necesarias para garantizar su funcionamiento seguro.

1. Introducción

1.1 Antecedentes

El nombre de la empresa es Bidaidea

La empresa se enfoca a consultoría y ciberseguridad de todo el funcionamiento de empresas para mantener protegidos sus sistemas informáticos, al igual que reducir amenazas y garantizar su correcto funcionamiento.

Los servicios que ofrece a sus clientes son:

- Clasificación y tratamiento de la Información
- Planes Estratégicos y directores
- Marcos de Controles y Normativos
- Análisis de Riesgos
- Simulacros de Crisis
- Definición e implementación de un PCN
- Homologación de Proveedores Críticos
- Planes de Prueba
- Planes de Gestión de Crisis

Atiende a empresas y negocios donde usen tecnologías de la información y dependan de estos para generar ingresos. Los clientes que atiende son en México y se están expandiendo a estados unidos.

Misión de la empresa:

Garantizar la seguridad de nuestros clientes y partners, brindándoles la mejor experiencia y prestando los servicios y productos de más alta calidad del mercado.

Nuestra misión es clara: Diseñar un futuro [ciber] seguro

1.2 Justificación

Las tareas y actividades que estaré realizando en el PAP se me hacen divertidas y me motivan mucho porque estoy aplicando conocimientos teóricos que adquirí en la carrera y por mi propia cuenta y sé que me servirán para irme abriendo camino en más ramas de la seguridad informática. En la carrera vimos y sigo viendo temas de administración de redes y servicios de red, al igual que la seguridad de estos. Durante la carrera todo era de práctica, pero ahora es un ambiente real con consecuencias reales, por lo que me siento más realizado y motivado ya que

realmente estoy aplicando los conocimientos aprendidos en la carrera, pero con responsabilidad.

Para llevar a cabo todos los deberes del PAP tengo programadas 15 horas por semana de investigación y descubrimiento de vulnerabilidades en la infraestructura del cliente y al mismo tiempo que realizo las actividades asignadas por el jefe del proyecto la cuales serán realizar monitoreo y conexiones entre varios centros de distribución, en el cual actuaré como administrador de firewall.

Como apoyo o recursos tendré tutorías de cómo realizar las tareas por parte del líder del proyecto en las áreas donde no esté muy seguro de llevar a cabo. También se me apoyará con resolución de dudas e inquietudes dentro del contexto del proyecto

La línea de negocio en la que estaré trabajando durante el PAP se me hace muy atractiva para desarrollarme profesionalmente ya que manejo conocimientos de redes y de seguridad al mismo tiempo.

1.3 Objetivos

Realizar colaboración activa con entidades de formativas para el desarrollo profesional de alumnado con el fin de poder captar talento antes de su comienzo en el mundo laboral

Espero obtener experiencia trabajando en equipo, aprender a utilizar las herramientas de trabajo usadas en este ámbito y aprender aspectos más humanos de empezar a trabajar en un ambiente laboral formal, ya sea saber pedir un aumento, decir no cuando una fecha de entrega sea muy corta, etc.

1.4 Contexto

El área operativa de la empresa es la de Ciberseguridad. El tipo de proyecto se enfocará en análisis de riesgos y planes Estratégicos y directores. Mi rol como estudiante realizando mi PAP será el de administrador de firewall e investigador de amenazas.

1.5 Entregables

Los entregables que debo producir en conjunto con mi equipo son Reportes de amenazas y vulnerabilidades.

Los entregables que debo producir personalmente son Resúmenes de credenciales y datos.

1.6 Involucrados

- Cliente de Bidaidea
- Líder del proyecto
- Miembros del equipo de trabajo

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

Inicio	Analizar la infraestructura del cliente e investigar posibles amenazas y vulnerabilidades.
Planificación	Líder de equipo decide el orden del trabajo y reparte las necesidades del cliente.
Ejecución	Realizar reportes y tareas correspondientes
Seguimiento y Control	Resolución de vulnerabilidades y amenazas. Realización de las necesidades del cliente.
Cierre	N/A

2.2 Sustento Teórico y Metodológico

Como metodología uso una metodología que propuso el líder del proyecto, ya que estamos dando mantenimiento continuo en un área cambiante donde repentinamente puede haber cambios en los sistemas en uso o cambios en los intereses del cliente.

2.3 Descripción del Proyecto

Mi equipo de trabajo y yo estaremos monitoreando los servicios y redes de los clientes para garantizar su seguridad, con el objetivo de proteger sus datos y operaciones. Para hacer esto llevaremos a cabo documentos mostrando las pruebas realizadas sobre las redes y servicios del cliente, mostrando los resultados buenos y malos, para posteriormente proponer soluciones y alternativas.

Mi proyecto PAP es en cascada, ya que se lleva a cabo un análisis seguida de una implementación y después mantenimiento y feedback. Este proyecto es independiente de otros módulos de la empresa. Algunas características de mi proyecto son el diseño e implementación de redes y el diseño de elaboración de casos de pruebas.

Las herramientas para producir los entregables del proyecto son:

Para las partes de descubrimiento de vulnerabilidades:

- Kali Linux

- Metasploit
- Nmap

Para las partes de administración de firewall:

- FortiCloud
- Fortinet

El alcance del proyecto se limita a generar los reportes y proponer soluciones del lado de ciberseguridad, mientras que del lado administrativo si tenemos acceso a los servicios activos y se espera que solucionemos problemas dentro de estos.

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	**Monitorización de amenazas**	2	2	0	4	A
1.1	Migración SIEM	1	1	0	3	A
1.2	Formación SIEM (Devo)	1	1	0	3	A
1.3	Administración SIEM	1	1	0	3	M
1.4	Sistema de alerta temprana	1	2	-1	3	A
1.5	Monitoreo de Alertas	2	3	-1	4	A
2	**Securización del dato**	2	2	0	3	A
2.1	Infraestructura respaldo de bajas	2	1	1	3	A
2.2	Sistema gestión de contraseñas	2	3	-1	3	A
3	**Securización de sistemas**	3	3	0	4	A
3.1	ISO Bastionada Windows 11	3	1	2	3	A
3.2	Bastionado de servidores Windows	3	1	2	3	A
4	**Seguridad en Red**	3	4	-1	4	A
4.1	Analisis vulnerabilidades públicas	3	3	0	4	A
4.2	Analisis vulnerabilidades internas	3	3	0	4	A
4.3	Adecuación políticas seguridad	3	3	0	4	A
4.4	Implementación MFA Firewalls	2	3	-1	4	A
4.5	Monitoreo tuneles IPSEC	2	2	0	3	A
5	**Despliegue de servicios**	1	3	-2	4	A
5.1	iKy OSINT Tool	1	3	-2	4	M

2.4 Plan de Trabajo

2.5 Equipo de Trabajo

Rol	*Responsabilidad*	*Nombre (opcional)*
Senior Cybersecurity Analyst	*Implementación y despliegue del proyecto*	*Andrés de la Poza*
Interns (equipo de investigación e implementación)	*Reportar vulnerabilidades y resolver problemas en la red.*	*(5 integrantes)*

2.6 Plan de Comunicaciones

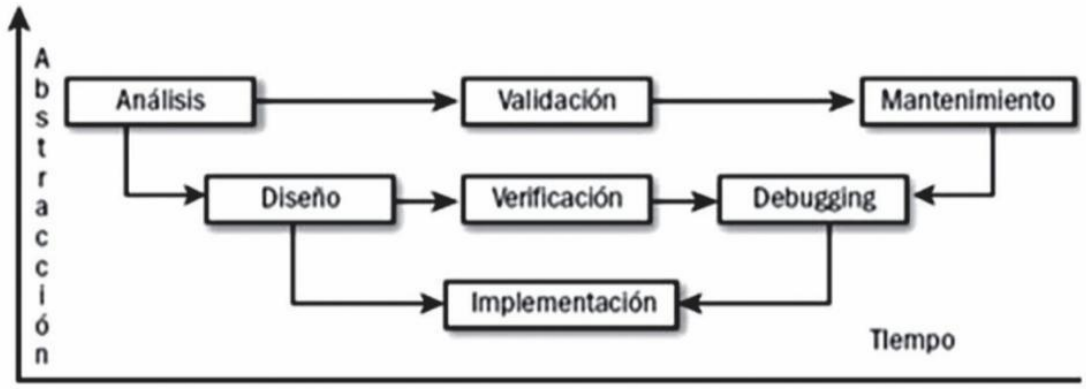
Emisor	*Mensaje*	*Receptor*	*Medio*	*Frecuencia*
Cliente	*Servicios y redes de la empresa*	*Líder del proyecto*	*Junta*	*Quincenal*
Líder del proyecto	*Asignación de tareas*	*Becarios*	*Videoconferencia*	*Diaria*
Becarios	*Reporte de análisis de amenazas*	*Líder del proyecto*	*Videoconferencia*	*Diaria*
Becarios	*Reporte de realización de tareas en el firewall*	*Líder del proyecto*	*Videoconferencia*	*Diaria*

2.7 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.*
Cliente	*Topología de red*	*Líder del proyecto*	*Topología completa*	*Realizar escaneos de esta*
Líder del proyecto	*Topología de red*	*Becarios*	*Topología completa*	*Repartir trabajo entre escaneos y cambios en el firewall*
Becarios	*Reportes de resultados*	*Líder del proyecto*	*Legibles y correctos*	*Preparar la información para presentar al cliente*
Líder del proyecto	*Reportes generales*	*Cliente*	*Presentación profesional*	*Tomar acciones necesarias.*

2.8 Seguimiento y Control

Se hacen juntas cada vez que se termina una carga de trabajo para discutir las acciones realizadas en la infraestructura existente, mientras que se hacen juntas semanales para presentar los reportes y discutir los hallazgos descubiertos en cuanto a los escaneos de vulnerabilidades. Con estas juntas se decide si se da por terminado un conjunto de actividades y si se deben tomar acciones correctivas antes de darlas por terminadas.



3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

1. Documentación de túneles IPSEC
2. Reporte de vulnerabilidades de la empresa XX
3. Reporte OSINT
4. Artículo de ciberseguridad

3.2 Estimación del Impacto

Los entregables que realicé en conjunto con mi equipo serán usados directamente para trabajar con los clientes, al igual que para promocionar la empresa ya que el artículo de ciberseguridad será compartido por la empresa para informar al publico de los peligros de los actuales virus que existen en la red.

5. Reflexiones del alumno

4.1 Aprendizajes Profesionales

- ¿Cuáles fueron las competencias técnicas que desarrollaste propias de tu profesión, así como las genéricas?

    1. Análisis vulnerabilidades públicas e internas
    2. Adecuación políticas seguridad

- ¿Cuáles fueron las competencias suaves que desarrollaste en tu participación PAP?

    1. Trabajo en equipo
    2. Comunicación
    3. Resolución de problemas

- ¿Cuáles fueron tus aprendizajes más importantes sobre el contexto sociopolítico y económico, y la problemática observada de tu campo profesional?

    Estoy aprendiendo la importancia de los ciberataques a nivel industrial ya que se ven afectados todos en la empresa y el problema se origina cuando las empresas no quieren invertir en ciberseguridad hasta que los atacan.

- ¿Cuáles fueron los saberes adquiridos en los estudios universitarios que fueron puestos a prueba en tu PAP?

    Mi habilidad para hacer troubleshooting fue puesta a prueba, al igual que mi conocimiento de redes y reglas de firewall.

4.2 Aprendizajes Sociales

- ¿Qué prácticas sociales y en qué ámbitos de la sociedad en los que crees que puedes innovar?

    Puedo innovar en la forma en la que la gente común practica la ciberseguridad y ser responsables en la red.

- ¿A qué grupos sociales benefició el proyecto?

El proyecto beneficia a las empresas y a todas las personas involucradas, ya que estas son el objetivo primario de los ciberataques.

- ¿Mis servicios profesionales produjeron bienes de carácter público?, cuáles?

  Mi conocimiento y comentarios a fondo acerca del tema de los virus en la industria pueden producir reflexión y causar que entidades terceras reconsideren aprovechar la oportunidad y adentrarse en la ciberseguridad.

- ¿Mis servicios profesionales contribuyen para mejorar la economía del país, o región?

  Mis servicios profesionales pueden ayudar a evitar que el gobierno pierda mas dinero y tiempo recibiendo ciberataques y vulnerabilidades.

4.3 Aprendizajes Éticos

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

  Encuentro similitudes en la responsabilidad y confianza que la empresa nos da a la hora de vulnerar y analizar la infraestructura de la empresa el cliente.

- ¿Identifico después de esta experiencia vivida, hacia dónde me lleva o invita en mi vida profesional y personal?

  Puedo identificar que esta experiencia me acerca al ambiente laborar rodeado por ciberseguridad y su aplicación en la configuración de redes laborales. Personalmente esta experiencia hizo que me interese aun más por los nuevos descubrimientos y hallazgos en el tema.

- ¿Me queda claro, cómo y para quien habré de ejercer mi profesión después de la experiencia del PAP?

  Aun no me queda muy claro que camino profesional quiero tomar después de este PAP, pero espero consolidarlo con el PAP número dos.

4.4 Aprendizajes Personales

¿La experiencia del PAP me dio elementos que ayudan para conocerme mejor, mis habilidades y mis potencialidades?

Este PAP me ayudó a saber en qué áreas me hace falta trabajar y en qué áreas se me da muy bien el realizar las cosas.

4.5 Tareas Aprendidas

a. ¿Cuáles fueron los factores, las acciones y/o las actitudes *(tuyas, líder, equipo)* que influyeron favorablemente para que se dieran los resultados exitosos del proyecto? El propósito es que los conozcas y documentes los factores que deben debes repetir en ocasiones futuras en tu desempeño profesional y personal.

Mi líder de equipo fue paciente y muy tranquilo a la hora de resolver dudas y demostrar como realizar cosas que no sabíamos.

Yo realicé todas las actividades con tiempo y si había algo que no sabia como hacer, se lo comunicaba a mi líder inmediatamente.

Mi equipo se repartió el trabajo priorizando las mejores cualidades y habilidades de cada uno.

b. ¿Cuáles fueron las situaciones, acciones y/o actitudes *(tuyas, líder, equipo)* 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? Esta reflexión te servirá para estos factores no pasen desapercibidos en ocasiones y proyectos futuros.

Nuestro líder pudo haber sido mas estricto con la presencia de los miembros para así tener más personas trabajando en el proyecto y aligerar la carga de trabajo.

5. Conclusiones

Puedo decir con certeza que esta experiencia PAP me ayudó mucho a dar el primero paso de estudiante a casi profesionista, aunque no sea un empleado todavía. Por primera vez tuve experiencia de primera mano con equipamiento y actividades de seguridad en redes de un negocio real, lo que permitió ver el peso y responsabilidad que cae en ingenieros como yo y el nivel de profesionalismo que se espera de mí.

El trabajar en equipo es muy importante en proyectos de gran escala, por lo que me agradó ver que mi equipo estuvo dispuesto a poner tiempo para ayudar cuando uno de mis compañeros cometió un error y desconfiguró una parte del trabajo, dándome a entender que es más importante ser transparente y honesto que intentar esconder mis errores yo solo por miedo a ser castigado.

Finalmente, me siento muy satisfecho con esta etapa, creo que los retos y desafíos presentados son muy interesantes y fácilmente me dan ganas de dedicar esfuerzo para lograr estos objetivos y metas. Creo que mis resultados son buenos y he ubicado las áreas a mejorar tanto técnicamente como profesionalmente.

6. Bibliografía y Anexos