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 TECNOLOGÍA I

BIDAIDEA GESTIÓN SL

PRESENTA

Alumno: ISI Luis Manuel Pérez Hernández

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

Para este trabajo se colaborará con diferentes entidades de formativas, todo para desarrollarme de forma profesional para lograr adquirir la mayor cantidad de información y conocimientos posibles con el fin de empezar dentro del mundo laboral con previa experiencia. Dentro de la empresa se tienen diferentes equipos, Red Team, Cloud Computing y Networking.

Estos equipos han analizado y reportado diferentes dispositivos, sitios web, y demás para mejorar la seguridad de los clientes. No solo se ha trabajado de manera repetitiva o tediosa, sino que también se han hecho investigaciones, análisis y documentación que ayuda a la empresa huésped y a los clientes de esta organización. Se muestra los productos entregados y el impacto que tiene el proyecto en la sociedad, el alumno y la empresa. Se tiene en claro qué habilidades se trabajaron, que aprendizajes y tareas se obtuvieron, y qué se puede concluir de todo esto.

1. Introducción

1.1 Antecedentes

Bidaidea Gestión SL

Consultoría, Sistemas y Ciberseguridad.

Bidaidea es una consultora multinacional, global, boutique e independiente. Entre sus líneas de negocio se encuentra la Ciberseguridad, Inteligencia y planes de seguridad física para Empresas y Pymes.

Tiene presencia en LATAM. EE. UU. y España.

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

Visión: Ser reconocidos como referentes en materia de ciberseguridad e Inteligencia en España y Latinoamérica, dando valor al conocimiento y experiencia de nuestros profesionales.

1.2 Justificación

En muchos momentos de la carrera me preguntaba cuándo podría a llegar a usar las habilidades y conocimientos adquiridos en las clases, dentro de las actividades en las que estaré trabajando se utilizan estos conocimientos y requieren que aprenda de otras cosas más específicas para lograrlo de la mejor manera, así adquiero más conocimiento de las bases aprendidas anteriormente.

Para poder realizar todo lo que se necesita dentro de las actividades requiero de un total de 19.5 horas a la semana para poder capacitarme de manera correcta y adquirir las competencias necesarias.

Para poder cumplir con los logros primeramente tendré acceso a los conocimientos de mi líder técnico, en segundo puesto, tendré acceso a dispositivos y sistemas de seguridad existentes para hacer pruebas o para trabajar en ellos. En tercer puesto laboratorios específicos para experimentar antes de implementar algún proyecto o tarea.

La línea de negocio en la que estoy me parece muy interesante y me atrae profesionalmente ya que puede ser un muy buen comienzo para mi carrera en seguridad informática.

1.3 Objetivos

El objetivo principal es 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 que profesionalmente pueda interactuar con diferentes personas en diferentes ramas de la empresa, para poder experimentar el trabajo corporativo, además, quisiera también entender mejor cómo funcionan las empresas de este tamaño interna e internacionalmente.

1.4 Contexto

Área de Ciberseguridad

Plan director de Seguridad

Analista/Consultor de Ciberseguridad.

1.5 Entregables

1. Reportes Evento
2. Documento de Configuración
3. Reporte de Monitoreo
4. Análisis OSINT Empresa
5. Reporte de Hito

1.6 Involucrados

- *Cliente externo*
- *Área de Seguridad Patrimonial (Interno del cliente)*
- *Jefe de Proyecto en España.*
- *Responsable en México*
- *Analista de Ciberseguridad (Alumno en Practicas)*

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

Inicio: Introducción al puesto, selección de horarios para los integrantes del grupo.

Planificación: Definición de roles, actividades y sub-equipos para actividades más específicas.

Ejecución: Investigación, reporte de investigación, configuración, reporte de configuración, despliegue y monitoreo.

Seguimiento: Mantenimiento y monitoreo de servicios, equipos y sistemas.

Control: Reportes de monitoreo.

Cierre: Reporte final.

2.2 Sustento Teórico y Metodológico

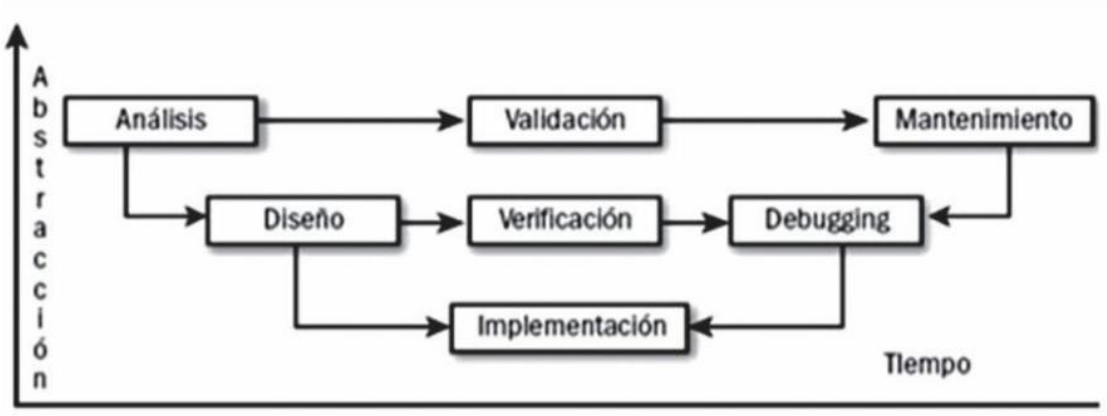
Para este proyecto se utilizará la metodología ágil ya que después de desplegar algún sistema o servicio se necesitará de monitoreo y actualizaciones, y con feedback de esto y otras cosas podremos actualizar el sistema, además de que, si el cliente lo requiere, se podrán hacer mejoras al servicio.

Dentro de Bidaidea se solicitará una investigación si el servicio lo requiere, y un reporte de la investigación, si no, se llega directo a la configuración, después un reporte de configuración, análisis de servicio, reporte de análisis y despliegue de nuevo sistema o actualización.

2.3 Descripción del Proyecto

Conocimiento y funcionamiento de redes en entornos corporativos, Conocer y entendimiento de Firewalls, reglas y configuración, comprensión completa de incidentes/logs, comprender y saber desarrollar desde la detección, investigación, análisis y subsanación de una alerta de ciberseguridad e Implementaciones de sistemas asociados a la ciberseguridad.

Para este proyecto PAP se usará un ciclo de vida en V, es muy usado para software, pero también sirve mucho para Análisis, Diseño, Implementación y Mantenimiento, aparte de que también se necesita feedback en el análisis y mantenimiento. Este ciclo es adaptable para proyectos de IT o de Ciberseguridad, ya que podemos ver mejoras, implementar cosas y mejorar el siguiente despliegue.



Estas competencias muestran lo que se necesita para ser muy bueno en el área de ciberseguridad pero que son cosas específicas igualmente, estas competencias diría que son básicas para alguien que trabaja en el área y para alguien avanzado como senior. La prioridad más alta es 5 lo que significa que para esta competencia debes tener mucha experiencia, la más baja es algo específico pero repetitivo y que puede llegar a ser tedioso, pero a la larga es fácil.

No.	Competencia	Nivel que tiene el Alumno	Nivel Requerido PAP	Objetivo al Final del PAP	Prioridad
1	Monitoreo de Amenazas	2	4	4	A
2	Protección de Datos	1	3	3	M
3	Protección de Sistemas	2	4	3	A
4	Seguridad de Redes	3	5	4	A
5	Servicios	2	4	3	M
6	Comunicación en inglés	3	4	4	B

2.4 Plan de Trabajo

No.	Actividad Educativa	Tipo Actividad	Prereq	Total Hrs	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Obj
1	**Monitoreo de Amenazas**																						
1.1	Migración SIEM	Trabajo Remoto		25	01/09/2022	30/09/2022																	
1.2	Formación SIEM (Devo)	Trabajo Remoto	1.1	10	15/09/2022	30/09/2022																	
1.3	Administración SIEM	Trabajo Remoto	1.2	35	19/09/2022	28/10/2022																	
1.4	Sistema de Alerta Temprana	Trabajo Remoto	1.3	10	19/09/2022	30/09/2022																	
1.5	Monitoreo de Alertas	Trabajo Remoto	1.4	20	01/09/2022	05/12/2022																	
2	**Protección de Datos**																						
2.1	Infraestructura Respaldo Bajas	Trabajo Remoto		25	03/10/2022	21/10/2022																	
2.2	Sistema Gestión de Contraseñas	Trabajo Remoto		20	24/10/2022	04/11/2022																	
3	**Protección de Sistemas**																						
3.1	ISO Bastionada Windows 11	Trabajo Remoto		25	07/11/2022	25/11/2022																	
3.2	Bastionado Servidores Windows	Trabajo Remoto		25	14/11/2022	05/12/2022																	
4	**Seguridad de Redes**																						
4.1	Análisis Vulnerabilidades Públicas	Trabajo Remoto		10	12/09/2022	11/11/2022																	
4.2	Análisis Vulnerabilidades Internas	Trabajo Remoto		15	13/09/2022	18/11/2022																	
4.3	Adecuación Políticas Seguridad	Trabajo Remoto		10	26/10/2022	25/11/2022																	
4.4	Implementación MFA Firewalls	Trabajo Remoto		15	03/10/2022	14/10/2022																	
4.5	Monitoreo Tuneles IPSEC	Trabajo Remoto		15	01/09/2022	05/12/2022																	
5	**Servicios**																						
5.1	Despliegue de IKy OSINT Tool	Trabajo Remoto		5	28/11/2022	05/12/2022																	
5.2	Despliegue de Laboratorio Ciberseguridad	Trabajo Remoto		20	14/11/2022	05/12/2022																	
5.3	Despliegue de Nessus	Trabajo Remoto		15	17/10/2022	28/10/2022																	
6	**Comunicación en Inglés**																						
6.1	Leer libros e investigar sobre las más	Autoestudio		15	29/08/2022	05/12/2022																	

2.5 Equipo de Trabajo

Rol	*Responsabilidad*	*Nombre (opcional)*
Senior Cybersecurity Analyst	*Implementación y despliegue del proyecto*	*Andrés de la Poza*
Cybersecurity Analyst	*Implementación y despliegue del proyecto*	*Alejandro Crespo*
Cybersecurity Analyst	*Implementación y despliegue del proyecto*	*León García*
Cybersecurity Analyst	*Implementación y despliegue del proyecto*	*Alejandro Rodríguez*
Cybersecurity Analyst	*Implementación y despliegue del proyecto*	*Pablo Zarate*

2.6 Plan de Comunicaciones

Emisor	*Mensaje*	*Receptor*	*Medio*	*Frecuencia*
Senior Analyst	*Información*	*Ciber Analysts*	*WhatsApp*	*s*
Ciber Analyst	*Entregable*	*Senior Analyst*	*WhatsApp/Plataforma Digital*	*s-2s*
Ciber Analyst	*Documento/Reporte*	*Senior Analyst*	*WhatsApp/Plataforma Digital*	*s-2s*
Profesor	*Información*	*Alumnos*	*Videoconferencia*	*2d/s*
Alumnos	*Documento*	*Profesor*	*Canvas*	*~2s*

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.*
Ciber Analyst	*Entregable*	*Senior Analyst*	*-Configuración correcta -Información pertinente -Conocimiento aplicado*	*Cliente actual*
Senior Analyst	*Retroalimentación*	*Ciber Analyst*	*-Eficiencia de comunicación*	*-*

2.8 Seguimiento y Control

Los seguimientos se hacen cada quince días, en caso de que el hito por fecha (plan) sea de importancia mayor los seguimientos se harán de manera semanal.

Dentro de las fechas de 22 de septiembre y el 6 de octubre se revisará el contenido del capítulo 1 y 2 del reporte, dentro de las fechas de 31 de octubre y el 14 de noviembre se revisará el contenido de los capítulos restantes del reporte. Por último, entre las fechas de 24 de noviembre y 1 de diciembre se revisará el video de la presentación final y el poster.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

1. Reporte OSINT Trusot
2. Reporte Análisis Reporte de Información Trusot
3. Reporte Análisis Reporte de Usuario Trusot
4. Configuración Túneles IPSEC cedis
5. Artículo Historia del Malware

3.2 Estimación del Impacto

Primero, los reportes OSINT, específicamente el que se hizo para Trusot será utilizado como referencia para otros análisis de vulnerabilidades externas, ya sea dentro de Bidaidea o para Trusot, podrán darse cuenta qué cosas no tienen que repetir y mantener seguras. En cuanto a reportes de Respaldo de Información, igualmente se puede usar como ejemplo para futuros análisis, especialmente el de Usuario, ya que nunca dejarán de tener personal que deje la empresa y siempre se necesita tener confidencialidad en esa área.

Los túneles IPSEC fueron configurados de la mejor manera posible, al no tener el completo control y monitoreo de estos, la configuración se hizo para que, en un futuro, las personas que tengan que monitorearlo o configúralo más sepan qué función tiene cada túnel y hacía donde los lleva, para una fácil configuración. Y, por último, aunque no es muy técnico, los artículos que como equipo estamos haciendo ayuda que las personas sean más conscientes de la seguridad que ellos, las empresas y las personas en general deben de tener y como ha evolucionado y siguen evolucionando.

4. Reflexiones del alumno
4.1 Aprendizajes Profesionales

Las competencias desarrolladas fueron:

- Seguridad en los servicios
- Protección de Datos
- Detección de Amenazas
- Trabajo en Equipo
- Investigación.

Creo que el contexto de mi área es demasiado grande, existe todavía un área muy gris en los campos donde se pueden hacer muchas cosas, es por esto por lo que se remunera de buena manera a los expertos en estas áreas. Aparte de que siempre se están diseñando maneras de romper la seguridad actual, cuando las empresas y personas se quedan atrás, es más fácil romper su seguridad.

Vulnerar de la manera que fuera las empresas y sus recursos, la investigación en Internet y Saberes técnicos.

Soy más capaz, no sabría que hacer al 100% pero definitivamente he mejorado las bases para evaluar de mejor manera y tomar la mejor decisión posible.

4.2 Aprendizajes Sociales

Compartir las vulnerabilidades encontradas, lo que puedo hacer para mejorar la sociedad es esforzarme lo más que pueda y compartir mis resultados para que todos tengan la posibilidad de estar seguros. Este proyecto beneficio a cualquier usuario que use el Internet.

Mi visión del mundo social cambió un poco, yo ya sabía cómo era el mundo de la ciberseguridad, pero de lo que va este semestre me he podido dar cuenta que hay mucho más de lo que sabía y que si quiero hacer algún impacto necesito esforzarme aún más.

El artículo "paper" me sirvió mucho para investigar cómo ha evolucionado la seguridad en Internet, como siempre la gente se la ingenia para descubrir nuevas cosas y como la tecnología avanza demasiado rápido para todos.

4.3 Aprendizajes Éticos

Mis valores personales son básicamente los mismos que el sentido social, lo que me agrada mucho. Me ha quedado más claro hacía donde quiero caminar, o correr, y que necesito esforzarme más si quiero sacarle provecho y dejar algo en mi camino que le sirva a los demás. Definitivamente elegí la carrera correcta, pero tengo que seguir aprendiendo.

4.4 Aprendizajes Personales

Ahora me conozco mejor, sé cuáles son mis habilidades y qué tanto puedo lograr a hacer, sé que cosas mejorar en estos momentos. Quería conocer el mundo laborar y como funciona, también cómo funcionan las personas dentro de este mundo, ahora me queda claro, pero creo que puedo aprender más cosas aún, probablemente cada que tenga una experiencia laboral diferente.

Creo que la experiencia del PAP me ayudó a identificar que no todo el mundo tiene las mismas habilidades y está bien no ser el mejor en una cosa, tengo mis propias habilidades y puedo ser útil si me lo propongo.

Todas las experiencias adquiridas me dieron nueva información, ahora puedo entender de diferente manera ciertas cosas y esto definitivamente me ayudará en mi vida profesional y personal.

4.5 Tareas Aprendidas

Definitivamente una para resultados exitosos fue querer aprender y usar los conocimientos adquiridos para resolver problemas, pero uno donde se puedo haber hecho de manera diferente fue al principio, ya que nos retrasamos un poco y el programa para que pudiéramos trabajar en un proyecto no estaba 100% definido y se puedo haber preparado mejor.

5. Conclusiones

Puedo concluir finalmente que es una experiencia completamente diferente a todo lo que he vivido, he tenido poca experiencia trabajando, pero igualmente fue algo totalmente diferente a eso anteriormente mencionado. Me di cuenta de que existe una jerarquía, una empresa con buena reputación y que tiene muchos trabajadores a su cargo hace muchas cosas todo el día todos los días y tu eres una parte pequeña que hacer funcionar todo. No todas las personas entienden de lo que estás hablando, tienes que pasar esa información de manera que todos lo puedan entender de la mejor manera.

Aprendí que te tienes que esforzar y hacer decisiones difíciles que requieren de información previamente revisada, especialmente en este campo, hay muchas personas que quieren llegar a la cima y si no trabajas y mejoras tus habilidades siempre habrá alguien que llegará antes que tú.

Pero también aprendí que no siempre tienes que estar estresado, se puede disfrutar de la vida y del trabajo, puedes mejorar tus habilidades y encontrar algo que te haga vivir de mejor manera. No todo es sí o no, hay muchas posibilidades y todos tenemos diferentes habilidades que podemos usar en diferentes cosas, solo es cuestión de hallarlas, pulirlas y trabajarlas.

Al final de todo puedo decir que estoy complacido por estas semanas que han pasado, espero poder aprender aún más en estas últimas semanas y espero con ansías el siguiente semestre para poder aprender aún más. Quiero llegar a mejorar mis habilidades y que pueda llegar lejos en mi vida personal y profesional.