

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
I, BIDAIDEA

PRESENTA

Alumno: ISI Pablo Gerardo ZÁRATE Félix

Profesor PAP: Juan Manuel Islas Espinoza, PMP®

Tlaquepaque, Jalisco, octubre de 2022.

ÍNDICE

Contenido

REPORTE PAP	2
Presentación Institucional de los Proyectos de Aplicación Profesional.....	2
Resumen	3
1. Introducción	4
1.1 Antecedentes	4
1.2 Justificación	4
1.2 Objetivos.....	5
1.3 Contexto	5
1.4 Entregables.....	5
1.5 Involucrados	5
2. Desarrollo del Proyecto PAP	7
2.1 Administración del Proyecto	7
2.2 Sustento Teórico y Metodológico	7
2.3 Descripción del Proyecto	8
2.4 Plan de Trabajo	9
2.5 Equipo de Trabajo.....	10
2.6 Plan de Comunicaciones	10
2.7 Plan de Calidad	10
2.8 Seguimiento y Control.....	10
3. Resultados del Trabajo Profesional	11
3.1 Productos Obtenidos	11
3.2 Estimación del Impacto	11
4. Reflexiones del alumno	12
4.1 Aprendizajes Profesionales	12
4.2 Aprendizajes Sociales.....	12
4.3 Aprendizajes Éticos.....	12
4.4 Aprendizajes Personales	13
4.5 Tareas Aprendidas	13
5. Conclusiones	14

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

Dentro del presente reporte voy a presentar de forma clara las características cruciales de mi proyecto PAP para el periodo de otoño 2022. Dentro del reporte podremos encontrar información sobre los objetivos del proyecto, calendarización de actividades, descripción del proyecto, entre otras.

La metodología que lleve a cabo para el desarrollo del proyecto conlleva el tomar notas de forma semanal con respecto a mis aprendizajes y opiniones del proyecto PAP, posteriormente regreso a estas notas para poder realizar los entregables solicitados por el profesor Juan Islas. De igual forma, una gran parte del reporte fue colaborativa, para la elaboración de estas partes nos reunimos internamente dentro de la empresa huésped con el objetivo de llegar a un acuerdo de la información que íbamos a presentar.

Al finalizar la lectura del reporte, el lector podrá ver el impacto del proyecto PAP en mi desarrollo como futuro ingeniero.

1. Introducción

A lo largo de este proyecto PAP formaremos parte de la empresa Bidaidea Gestión SL con el rol de internos, formaremos parte de un proyecto de auditoría e implementación de soluciones para una empresa cuyo giro es aquel del retail.

El proyecto consta de cinco fases, a lo largo de las cuales realizaremos diversas actividades que deberemos reportar a nuestro líder de proyecto, así como nuestros hallazgos durante dichas actividades.

1.1 Antecedentes

Bidaidea Gestión SL, es una consultora multinacional, global, boutique e independiente Tecnología para un mundo más Ciberseguro. 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. Atiende a las necesidades de ciberseguridad de empresas de diversos giros.

1.2 Justificación

La razón por la cual me interesa formar parte de este proyecto PAP es que al poder trabajar en una empresa privada, nos damos cuenta de todos los procesos que se tienen que seguir al trabajar como consultores externos para empresas privadas, encuentro dichos aprendizajes muy valiosos y creo es crucial tener un buen entendimiento de los procesos al iniciar mi carrera como ingeniero.

Para este proyecto PAP debemos de dedicar 20 horas de esfuerzo a la semana, sin embargo, el líder de proyecto maneja objetivos que se tienen que cumplir independientemente del tiempo, por lo que sí toma más o menos de 20 horas no tiene tanta relevancia, lo importante es cumplir el objetivo.

La empresa huésped nos ha facilitado clases en video conferencia, así como cursos en línea, todos relacionados con la ciberseguridad y el desarrollo de habilidades interpersonales. De igual forma tenemos la libertad de consultar dudas y recibir mentorías por parte del líder del proyecto.

La industria privada es una línea de negocio que me resulta interesante y retadora para mi futuro como ingeniero.

1.3 Objetivos

El objetivo de la empresa es acompañar a las diferentes organizaciones en materia de estrategia y la transformación digital de la Seguridad Integral.

Tengo como objetivo finalizar mi proyecto PAP con una visión más amplia de las redes corporativas y sus entornos tecnológicos, así como analizar y adaptarme a las metodologías y procesos que usan las empresas para el área de tecnologías.

1.4 Contexto

Se realizará una auditoria sobre la empresa cliente con el propósito de identificar las áreas de mejora. Una vez identificadas, se implementarán las medidas de seguridad necesarias para que la empresa cliente pueda pasar la certificación ISO 27001.

Los procesos de investigación y mejora se realizan completamente sobre la infraestructura existente de la empresa cliente.

La empresa huésped opera en las ramas de la Ciberseguridad, Inteligencia y planes de seguridad física para Empresas y Pymes. Mi rol dentro de la empresa es de interno, dónde estaremos involucrados en todas las fases de auditoría y documentación.

1.5 Entregables

- Reportes de hallazgos
 - Al momento de que los internos encontremos brechas de seguridad dentro de la organización, deberemos de realizar un reporte en dónde describamos claramente cómo la encontramos y el plan de mitigación.
- Solicitud de cambios
 - Cuando los internos deseemos realizar cambios en la infraestructura del cliente, deberemos de realizar una solicitud de cambio que tiene que ser aprobada por los lideres del proyecto. Dicha solicitud debe contener información del cambio a realizar, en dónde y cuándo.
- Documentación de proceso
 - En caso de implementar nuevos procesos, debemos de documentarlos para que exista transferencia de conocimiento a los futuros empleados de la compañía.

1.6 Involucrados

- Cliente externo.
- Líder del Proyecto.
- Internos

2. Desarrollo del Proyecto PAP

Se realizará una auditoria sobre la empresa cliente con el propósito de identificar las áreas de mejora. Una vez identificadas, se implementarán las medidas de seguridad necesarias para que la empresa cliente pueda pasar la certificación ISO 27001.

Los procesos de investigación y mejora se realizan completamente sobre la infraestructura existente de la empresa cliente.

2.1 Administración del Proyecto

La administración del proyecto PAP la lleva a cabo el líder del proyecto, el cual es el encargado de dar por iniciadas u finalizadas las diferentes etapas del proyecto.

Al inicio del proyecto PAP recibimos las instrucciones del proyecto y la dinámica que tendríamos como equipo. En las sesiones posteriores fuimos parte de la planificación de actividades, dentro de dichas sesiones nos comentaron el plan de acción y la calendarización de actividades.

La presente etapa es la de ejecución, dentro de esta etapa estamos realizando las labores de auditoría e implementación de estándares de seguridad, durante esta etapa nos encargamos de buscar las brechas de seguridad, documentarlas, comunicarlas a cliente y proceder con la solución a dichas brechas.

Las etapas de seguimiento y control serán necesarias para validar el correcto funcionamiento de las soluciones implementadas, una vez hayan sido validadas las soluciones podremos proceder con el cierre del proyecto.

2.2 Sustento Teórico y Metodológico

Estaremos trabajando con una metodología de ciclo V, cuyas fases podemos observar en la siguiente imagen.



Dada la naturaleza del proyecto, la etapa de implementación conlleva una fase de mantenimiento de la cuál pueden surgir mejoras que posteriormente inician el ciclo nuevamente

2.3 Descripción del Proyecto

Actualmente formo parte de un proyecto de auditoría de seguridad, dicho proyecto consiste en analizar el ciberespacio de una empresa privada con el propósito de encontrar y solucionar las brechas de seguridad que encontremos. El objetivo final del proyecto es dejar una infraestructura segura que cumpla todos los estándares de calidad necesarios para conseguir la certificación ISO 27001.

El ciclo de vida del proyecto es iterativo, ya que después de cada implementación debemos de regresar para su mantenimiento; después de dicho mantenimiento pueden surgir mejoras que inicien nuevamente el ciclo de validación. Dentro de cada fase del proyecto debemos de realizar reportes de hallazgos, esto consiste de documentar la forma en la que encontramos la brecha, como se va a solucionar, causa raíz de la brecha de seguridad, cuándo la descubrimos y cuándo se espera quede solucionada.

Dentro de este proyecto tendré la oportunidad de mejorar mis habilidades de arquitectura de redes corporativas, auditoría de seguridad y seguridad en redes; dichas habilidades son cruciales para el óptimo desarrollo del proyecto y sin duda tendrán un impacto duradero en mi carrera.

Los recursos tecnológicos que estaré usando para producir los entregables serán herramientas como FortiCloud, la cual es una consola de administración de dispositivos pertenecientes a la empresa cliente, de aquí podré importar los datos necesarios para mi reporte, posteriormente podremos hacer análisis de datos con MS Excel y por último realizar el reporte en sí con MS Word.

El alcance de mi proyecto educativo contempla las siguientes competencias:

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	Análisis vulnerabilidades públicas	3	3	0	4	A
4.2	Análisis 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

PROYECTOS Y ACCIONES	PLAN DE ACCIÓN															
	SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Monitorización de Amenazas	[Redacted]															
Migración SIEM	[Redacted]															
Formación SIEM (Devo)	[Redacted]															
Administración SIEM	[Redacted]															
Sistema de Alerta Temprana	[Redacted]															
Monitoreo de Alertas	[Redacted]															
Securización del Dato	[Redacted]															
Infraestructura Respaldo Bajas	[Redacted]															
Sistema Gestión de Contraseñas	[Redacted]															
Securización de Sistemas	[Redacted]															
ISO Bastionada Windows 11	[Redacted]															
Bastionado Servidores Windows	[Redacted]															
Seguridad en Red	[Redacted]															
Análisis Vulnerabilidades Públicas	[Redacted]															
Análisis Vulnerabilidades Internas	[Redacted]															
Adecuación Políticas Seguridad	[Redacted]															
Implementación MFA Firewalls	[Redacted]															
Monitoreo Tuneles Ipsec	[Redacted]															
Despliegue de Servicios	[Redacted]															
iKy OSINT Tool	[Redacted]															
Laboratorio Ciberseguridad	[Redacted]															
Despliegue de Nessus	[Redacted]															

Proyecto educativo	Duración del proyecto															
	Septiembre				Octubre				Noviembre				Diciembre			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1. Ethical Hacking	[Redacted]															
1.1 Tomar curso	[Redacted]															
1.2 Realizar practicas en linea	[Redacted]															
2. ITSM	[Redacted]															
2.1 Tomar curso	[Redacted]															
2.2 Realizar prácticas de los procesos de ITSM	[Redacted]															
3. Soft skills	[Redacted]															
3.1 Charlar con lideres del proyecto	[Redacted]															
3.2 Tomar cursos	[Redacted]															

2.5 Equipo de Trabajo

<i>Rol (#)</i>	<i>Responsabilidad</i>	<i>Nombre (opcional)</i>
<i>Senior Cybersecurity Analyst</i>	<i>Implementación y despliegue del proyecto</i>	<i>Andrés de la Poza</i>
<i>Interns</i>	<i>Implementación y despliegue del proyecto</i>	<i>(5)</i>

2.6 Plan de Comunicaciones

<i>Emisor</i>	<i>Mensaje</i>	<i>Receptor</i>	<i>Medio</i>	<i>Frecuencia</i>
<i>Líder del proyecto</i>	<i>Inicio y finalización de etapas</i>	<i>Internos</i>	<i>Video conferencia</i>	<i>Varia</i>
<i>Interno</i>	<i>Entregables y reportes</i>	<i>Líder del proyecto</i>	<i>Correo electrónico</i>	<i>Varia</i>
<i>Interno</i>	<i>Dudas</i>	<i>Líder del proyecto</i>	<i>Video conferencia</i>	<i>Varia</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>Líder del proyecto</i>	<i>Etapas del proyecto</i>	<i>Alejandro Crespo</i>	<i>Según corresponda al líder</i>	<i>Internos</i>
<i>Interno</i>	<i>Entregable</i>	<i>Líder del proyecto</i>	<i>Revisión del funcionamiento y configuración</i>	<i>Departamento de Tecnologías de la información</i>
<i>Interno</i>	<i>Reporte</i>	<i>Líder del proyecto</i>	<i>Contenido del reporte, así como descripción de las herramientas a utilizar</i>	<i>Líder del proyecto</i>
<i>Interno</i>	<i>Información</i>	<i>Líder del proyecto</i>	<i>Links de fuentes validas y sustentadas</i>	<i>Líder del proyecto</i>

2.8 Seguimiento y Control

Durante la etapa de seguimiento y control, el líder de proyecto nos reúne a todos en una videoconferencia dentro de la cual todos los internos presentamos los avances y hallazgos con respecto al proyecto. Estas sesiones se realizan de forma semanal, dependiendo de los avances y estado actual del proyecto, puede que haya ciertas modificaciones al calendario de actividades. Lo ideal es no incurrir en retrasos y continuar con todas las actividades tal cual fueron planeadas desde un inicio.

Frente a la coordinación PAP, estaré encargado de entregar reportes dentro de los cuales describa las actividades realizadas y aprendizajes adquiridos a lo largo de mi

proyecto PAP, dicho reporte será revisado por el profesor para posteriormente recibir retroalimentación. En base a la retroalimentación del profesor, deberé de generar cambios en mi documento con tal de que el reporte final que se presente a la coordinación PAP cumpla con los estándares de calidad esperados para un estudiante universitario.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

1. Análisis OSINT
2. Reporte OSINT
3. Artículo de ciberseguridad

3.2 Estimación del Impacto

El propósito del análisis y posterior reporte OSINT era poder presentar de forma clara y concisa un resumen con el que el cliente pueda darse una idea clara de toda la información que tiene pública y de libre acceso. Muchas veces cuando los clientes manejan diversos sitios pueden perder el registro de la información que publican y accidentalmente podrían exponer más información de la necesaria.

Es ahí donde resalta la importancia de un reporte como el realizado por el equipo de Bidaidea; Ya que le ahorra al cliente la labor de recopilar y organizar información. Gracias a este reporte, el cliente puede tomar acción ágil y efectiva con respecto a la información que pudiera representar un posible compromiso.

El artículo de ciberseguridad tiene una trascendencia un tanto más complejo, ya que al ser un artículo escrito con el propósito de la divulgación, este puede ayudar a cualquier persona que desee averiguar un poco más sobre la ciberseguridad, así como también ayudar a Bidaidea con sus presentaciones de ventas, capacitaciones, etc.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

Competencias técnicas:

- Implementación y administración de firewalls
- Implementación y administración de VPN's
- Documentación de hallazgos
- Investigaciones de clientes vía OSINT y Ethical Hacking

Competencias suaves:

- Trabajo en equipo
- Administración del tiempo
- Comunicación
- Resolución de problemas
- Toma de decisiones

4.2 Aprendizajes Sociales

Yo considero que mis practicas profesionales no solo tuvieron beneficios dentro de la iniciativa privada, dado que al nosotros realizar un artículo de divulgación ponemos nuestro conocimiento al servicio de los demás.

Mi visión respecto a la divulgación de conocimiento cambio, me he dado cuenta de la importancia que tiene la ciberseguridad en la sociedad actual y el impacto que puede tener en las vidas de las personas. Al nosotros compartir información de ciberseguridad de forma clara, podemos ayudar a que la gente de nuestro alrededor prevenga posibles ataques informáticos o que simplemente sean más conscientes con respecto a sus datos y el cómo se manejan por el internet.

4.3 Aprendizajes Éticos

A lo largo de mis prácticas profesionales, nunca experimenté algún tipo de conflicto con mis valores personales. Considero que la industria de la cual formé parte se maneja bajo rigurosos estándares éticos debido a lo delicado que es trabajar con la información de las personas.

He notado que, dentro de la industria de la ciberseguridad, tener principios firmes es clave para poder seguir avanzando y tener un buen desarrollo profesional.

4.4 Aprendizajes Personales

El haber tenido una experiencia profesional dentro de una empresa extranjera me ha dejado muchos aprendizajes personales, valoro la diversidad en los ambientes laborales y considero que enriquece a las empresas. Sin duda el haber formado parte de estas prácticas profesionales me ha ayudado a desarrollar mis habilidades interpersonales en entornos profesionales.

4.5 Tareas Aprendidas

Una buena comunicación fue clave para el óptimo desarrollo de mis prácticas profesionales, considero que, al tratarse de una primera experiencia laboral, la empresa huésped no esperaba que supiéramos todo, noté que lo más importante para ellos era que tuviéramos una buena integración como equipo de trabajo para así poder realizar nuestras actividades de forma más efectiva.

Considero que, para mis futuras experiencias laborales, el factor más importante seguirá siendo el poder trabajar en equipo y mantener la buena comunicación.

En cuanto a las actitudes que necesito mejorar, identifiqué que hay situaciones en las que necesito ser proactivo para la planificación de reuniones y discusiones del proyecto, dado que así pudiera agilizar mis tareas y las de mi equipo.

5. Conclusiones

Terminando este ciclo de prácticas profesionales, me voy satisfecho con lo aprendido y considero que las lecciones aprendidas a lo largo de este curso me serán útiles por el resto de mi carrera.

Considero que fue una buena experiencia laboral ajustada a las nuevas condiciones postpandemia, el trabajo remoto y desarrollo de proyectos con personas al otro lado del mundo ha sido de gran ayuda para conocer las herramientas y metodologías para realizar el trabajo de forma efectiva.