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

PRESENTA

Alumno: ISI Rafael Alejandro CRESPO Osuna

Profesor PAP: Juan Manuel Islas Espinoza, PMP®

Tlaquepaque, Jalisco, 5 de 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

El proyecto PAP al que estoy participando trata de hacer investigación y mejora sobre la infraestructura existente de las empresas que contratan a Bidaidea de acuerdo con mejorar su gobernanza y control de la infraestructura de los clientes externos que contrataron a Bidaidea para ello.

El alcance de los resultados es distinto y varía para cada empresa, pero se pudiera poner en común las actividades de la auditoría y revisión del estado de la red para proponer mejoras y haciendo cumplimiento de la ISO 27001, así como la creación de reportes para mostrar los resultados de las auditorías y del impacto que tendría dejar la infraestructura sin cambios y con vulnerabilidades en la red.

1. Introducción

1.1 Antecedentes

El nombre de la organización huésped donde estoy haciendo las prácticas es Bidaidea. Bidaidea es una empresa internacional la cual brinda cuatro servicios que son consultoría, sistemas, ciberseguridad y formación. Sus principales mercados son aquellas empresas que simplemente requieran de alguno de los servicios mencionados anteriormente para su misma empresa. Ya sea una consultoría para corroborar que el diseño de su red, estrategias integrales y/o planes de emergencia estén implementados de manera óptima; Soluciones CCTV, control de accesos, megafonía, interfonía y gestión de seguridad; Servicios de ciberseguridad para construir negocios resilientes y formación de calidad en extinción de incendios. Tiene presencia en LATAM, EEUU y España.

Identificaría la sinceridad, la honestidad y la responsabilidad como valores ya que es una empresa que se compromete con los clientes para brindarles el mejor servicio de seguridad en su infraestructura. Su objetivo sería acompañar a las diferentes organizaciones en materia de estrategia y la transformación digital de la Seguridad Integral.

1.2 Justificación

Las razones que me motivarán para invertir mi esfuerzo en un PAP de estas características será que principalmente descubriré y entenderé como es el ambiente laboral en una empresa tecnológica, el poder aplicar los conocimientos adquiridos a lo largo de la carrera. Además, que aprenderé aspectos técnicos más específicos, como tecnologías de alguna marca que estén utilizando o vayan a implementar. Esto servirá muy bien para ir creando mi historial e ir completando mi curriculum y mi perfil en LinkedIn. La relación que encuentro entre las actividades y compromisos de adquiero con la formación que he tenido en mi carrera es que en la carrera vemos las bases y el procedimiento inicial para la configuración o instalación de algo, en la empresa ya dan por hecho que sabes de ese tema o el principio de este.

Deberé intervenir un mínimo de 20 horas semanales a este PAP, esto para tener tiempo de capacitarme y adquirir las competencias necesarias, pero sin dejar a un lado las materias que estoy cursando en este semestre.

Una facilidad será que al ser home office al 100%, por lo que no perderé tiempo en traslados. Dado que utilizo mi computadora personal para conectarnos remotamente a los ambientes de trabajo como a las videollamadas, tengo todo a la mano en un mismo lugar por si tengo que salir de casa o del ITESO. La persona encargada del proyecto en Bidaidea es alguien que genera confianza y apoya mucho, por lo que entiende si tenemos algún pendiente de alguna entrega escolar.

Esta línea de negocio me resulta muy atractiva para desarrollarme cuando me gradúe ya que es un área relativamente nueva y existe mucho trabajo al respecto además de mucha demanda laboral.

1.3 Objetivos

Para mí, los propósitos de la empresa huésped es capacitar alumnado para que al final, si el alumno gusta y existe algún cupo en la empresa, el alumno pueda seguir trabajando en la empresa fuera del contexto PAP y captar el talento antes de nuestro comienzo en el mundo laboral. Esto porque ya se demostró el conocimiento y existe interés por parte del alumno.

Los objetivos que espero durante mi participación en este periodo es aprender lo más posible sobre herramientas y la forma de trabajar en un ambiente empresarial. Con la presión que existe del trabajo bajo presión y el saber que, si configuramos de manera errónea o incompleta alguna parte, podemos dejar sin servicio momentáneamente a la empresa.

1.4 Contexto

La empresa se encuentra en el departamento o área operativa de ciberseguridad. Dentro de las competencias de dicho plan se realizará un análisis de GAP sobre cumplimiento de la ISO 27001, revisión del estado de la red y una auditoría de seguridad que conforman los "hitos" del proyecto. El proyecto contendrá procesos de investigación y mejora sobre la infraestructura existente de acuerdo con mejorar su gobernanza y control de su infraestructura.

El rol que tendré será como solamente becario, en la primera junta se nos comentó que no nos exigirán tanto ya que sólo tenemos este rol, pero si estaremos en los procesos para aprender y aportar lo necesario. Los entregables que se espera producir son:

- Sistema de Alertas.
- Implementación de MFA Firewalls.
- Infraestructura de respaldo de bajas.

1.5 Entregables

Los entregables se irán produciendo en equipo durante este periodo PAP. Entre ellos se encuentra la monitorización de amenazas de la empresa a la que estaremos trabajando, con esto se realizará una migración, formación y administración del sistema SIEM. También generaremos una infraestructura para el respaldo de las

bajas que se generen en la empresa que nos contrató, así como un sistema de gestión de contraseñas. Para el apartado de seguridad en la red realizaremos análisis de vulnerabilidades públicas e internas, con esto realizaremos adecuaciones a las políticas de seguridad y realizaremos monitoreos a túneles ipsec. Se harán despliegues de servicios usando las herramientas de OSINT e iKy, se intentará crear un laboratorio de ciberseguridad para la realización de pruebas antes de implementarse en el entorno funcional.

Involucrados

La persona interesada directamente a los resultados del proyecto será el líder del proyecto que además es quien aprobará los entregables. Para la producción de los entregables los responsables serán los miembros del equipo de trabajo, yo estaré dentro de este rol junto con mis compañeros del PAP.

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

Para la administración del proyecto, se describe el inicio para sentar cuáles serán las bases de investigación, los roles con las tareas correspondientes para los integrantes del equipo y en que horarios se realizarán las tareas mencionadas. En el apartado de planificación el líder del equipo da las pautas para las investigaciones correspondientes para tecnologías en específico. En ejecución se realizan los reportes correspondientes a las actividades realizadas y descubrimientos. Para el apartado de seguimiento y control, se hace la realización de las minutas necesarias antes de pasarlas al documento final. Para el cierre no procede todavía al alcance del proyecto.

2.2 Sustento Teórico y Metodológico

Se trabaja con metodología ciclo en V que basa su principio en la gestión secuencial y lineal, pero con subfases de debug. Se utiliza esta metodología ya que cualquier cambio o implementación tiene su parte de mantenimiento, del cual se pueden implementar mejoras. Así como desde la fase de análisis podemos ver mejoras a implementar a nuestro despliegue.

2.3 Descripción del Proyecto

El tipo de proyecto que es mi PAP es acerca de la ciberseguridad en las empresas que han pedido ayuda a la empresa donde estoy. Bidaidea les brinda el servicio de consultoría para mejorar el diseño y seguridad de sus redes. El equipo donde estoy se encarga de apoyar esta mejora aplicando los conocimientos adquiridos a lo largo de la carrera. El proyecto PAP forma parte de un proyecto independiente dentro de la empresa bidaidea, por lo que no estamos al cien por ciento dentro de todas las operaciones.

Una clasificación más específica del proyecto es el uso de herramientas para determinar si la información de la empresa cliente es vulnerable al mal uso de las personas, por lo que se debe cambiar esa configuración que tienen, realizar nuevas pruebas y así determinar la seguridad de algún sitio o aplicación móvil.

Como los recursos tecnológicos se encuentran de manera remota, solo es necesario tener una computadora con acceso a internet para tener una conexión remota a estos dispositivos, además de una herramienta para el uso de contraseñas de los dispositivos. Además de esto, es necesario un medio de comunicación del equipo de trabajo con el líder de proyecto para las notificaciones de reuniones, dudas o lo que se requiera.

Los recursos que son utilizados para producir los entregables del proyecto es principalmente el editor de textos Microsoft Word, donde se desarrolla las características y los descubrimientos de la tarea; y Power Point para la presentación de resultados para la organización cliente.

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	**Monitorización de Amenazas**	4	0	4	4	M
1.1	Migración SIEM	4	0	4	4	M
1.2	Formación SIEM	4	0	4	4	M
1.3	Administración SIEM	4	0	4	4	B
1.4	Sistema de Alerta Temprana	4	0	4	4	A
1.5	Monitoreo de Alertas	4	0	4	4	A
2	**Securización del Dato**	5	2	3	5	M
2.1	Infraestructura Respaldo Bajas	5	2	3	5	A
2.2	Sistema de Gestión de Contraseñas	5	2	3	5	A
3	**Securización de Sistemas**	4	2	2	5	M
3.1	ISO Bastionada Windows 11	4	2	2	5	M
3.2	Bastionado Servidores Windows	4	2	2	5	M
4	**Seguridad en Red**	5	3	2	5	M
4.1	Análisis de Vulnerabilidades Públicas	5	2	3	5	A
4.2	Análisis de Vulnerabilidades Internas	5	2	3	5	A
4.3	Adecuación Políticas de Seguridad	5	3	2	5	M
4.4	Implementación MFA Firewalls	4	2	2	5	M
4.5	Monitoreo Tuneles Ipsec	4	1	3	5	B
5	**Despliegue de Servicios**	3	1	2	4	M
5.1	iKy OSINT Tool	4	2	2	4	M
5.2	Laboratorio de Ciberseguridad	4	2	2	4	M
5.3	Despliegue de Nessus	3	0	3	4	M

2.4 Plan de Trabajo

Plan resumido del PAP.

No.	Topic	Start Date	Finish Date	Dependency	Stakeholder	Total Hrs
1	**Monitorización de Amenazas**				**Andrés de la Poza**	139
1.1	Colaborar para hacer la migración de SIEM en la empresa.	1 de septiembre	30 de septiembre			
1.2	Colaborar para hacer la formación de SIEM en la empresa.	15 de septiembre	30 de septiembre			
1.3	Revisar que las adaptaciones de SIEM se hayan realizado correctamente asi como la administración de la misma.	21 de septiembre	31 de octubre	1.3		
1.4	Configuración e implementación de un sistema de alerta temprana.	21 de septiembre	7 de octubre			
1.5	Realizar un monitoreo sobre las alertas que se hayan levantado y hacer las acciones correspondientes según sea la gravedad.	1 de septiembre	5 de diciembre			
2	**Securización del Dato**				**Andrés de la Poza**	14
2.1	Revisar y ajustar la infraestructura de respaldo de bajas de la empresa.	1 de octubre	31 de octubre			
2.2	Configuración del sistema de gestión de contraseñas.	21 de octubre	7 de noviembre			
3	**Securización de Sistemas**				**Andrés de la Poza**	16
3.1	Hacer uso e instalación de la ISO bastionada para Windows 11	8 de noviembre	30 de noviembre			
3.2	Realizar bastionado de los servidores Windows.	15 de noviembre	7 de diciembre			
4	**Seguridad en Red**				**Andrés de la Poza**	88
4.1	Realizar un análisis de vulnerabilidades públicas.	7 de septiembre	14 de septiembre			
4.2	Realizar un análisis de vulnerabilidades internas.	7 de septiembre	21 de septiembre			
4.3	Realizar una adecuación de las políticas de seguridad.	22 de septiembre	30 de septiembre	4.1 y 4.2		
4.4	Hacer una implementación MFA sobre los Firewalls.	1 de octubre	14 de octubre			
4.5	Realizar un monitoreo de los túneles Ipsec.	1 de septiembre	5 de diciembre			
5	**Despliegue de Servicios**				**Andrés de la Poza**	39
5.1	Hacer uso de las herramientas iKy OSINT Tool.	1 de diciembre	5 de diciembre			
5.2	Levantar un laboratorio de ciberseguridad para la realización de pruebas internas.	15 de noviembre	5 de diciembre			
5.3	Hacer un despliegue del escaenr de vulnerabilidades Nessus.	15 de octubre	31 de octubre			

Plan de actividades educativas.

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	**Monitorización de Amenazas**			139																			
1.1	Colaborar para hacer la migración de SIEM en la empresa.	Autoestudio /Tutoría		16	1 de septiembre	30 de septiembre																	
1.2	Colaborar para hacer la formación de SIEM en la empresa.	Autoestudio /Tutoría		12	15 de septiembre	30 de septiembre																	
1.3	Revisar que las adaptaciones de SIEM se hayan realizado correctamente asi como la administración de la misma.	Autoestudio	1.3	36	21 de septiembre	31 de octubre																	
1.4	Configuración e implementación de un sistema de alerta temprana.	Autoestudio /Tutoría		10	21 de septiembre	7 de octubre																	
1.5	Realizar un monitoreo sobre las alertas que se hayan levantado y hacer las acciones correspondientes según sea la gravedad.	Autoestudio		65	1 de septiembre	5 de diciembre																	
2	**Securización del Dato**			14																			
2.1	Revisar y ajustar la infraestructura de respaldo de bajas de la empresa.	Autoestudio /Tutoría		8	1 de octubre	31 de octubre																	
2.2	Configuración del sistema de gestión de contraseñas.	Autoestudio		6	21 de octubre	7 de noviembre																	
3	**Securización de Sistemas**			16																			
3.1	Hacer uso e instalación de la ISO bastionada para Windows 11	Autoestudio /Tutoría		6	8 de noviembre	30 de noviembre																	
3.2	Realizar bastionado de los servidores Windows.	Autoestudio		10	15 de noviembre	7 de diciembre																	
4	**Seguridad en Red**			88																			
4.1	Realizar un análisis de vulnerabilidades públicas.	Autoestudio		8	7 de septiembre	14 de septiembre																	
4.2	Realizar un análisis de vulnerabilidades internas.	Autoestudio		8	7 de septiembre	21 de septiembre																	
4.3	Realizar una adecuación de las políticas de seguridad.	Autoestudio	4.1 y 4.2	4	22 de septiembre	30 de septiembre																	
4.4	Hacer una implementación MFA sobre los Firewalls.	Autoestudio /Tutoría		8	1 de octubre	14 de octubre																	
4.5	Realizar un monitoreo de los túneles Ipsec.	Autoestudio		60	1 de septiembre	5 de diciembre																	
5	**Despliegue de Servicios**			39																			
5.1	Hacer uso de las herramientas iKy OSINT Tool.	Autoestudio		6	1 de diciembre	5 de diciembre																	
5.2	Levantar un laboratorio de ciberseguridad para la realización de pruebas internas.	Autoestudio /Tutoría		25	15 de noviembre	5 de diciembre																	
5.3	Hacer un despliegue del escaenr de vulnerabilidades Nessus.	Autoestudio /Tutoría		8	15 de octubre	31 de octubre																	

2.5 Equipo de Trabajo

Rol (#)	*Responsabilidad*	*Nombre (opcional)*
1	*Jefe de proyecto*	*Andrés de la Poza*
2	*Compañero de proyecto*	
2	*Compañero de proyecto*	
2	*Compañero de proyecto*	
2	*Compañero de proyecto*	

2.6 Plan de Comunicaciones

Emisor	*Mensaje*	*Receptor*	*Medio*	*Frecuencia*
Líder del Proyecto	*Instrucciones*	*Becarios*	*Discord*	*Semanal*
Becario	*Información*	*Líder de Proyecto*	*WhatsApp*	*Semanal*
Becario	*Configuraciones*	*Líder de Proyecto*	*Discord*	*Semanal*
Becario	*Reporte*	*Líder de Proyecto*	*WhatsApp*	*Quincenal*
Becario	*Documento*	*Líder de Proyecto*	*WhatsApp*	*Quincenal*

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.*
Líder del Proyecto	*Etapa del proyecto*	*Yo*	*Según corresponda al líder.*	*Becarios*
Becario	*Entregable*	*Líder del Proyecto*	*Revisión de funcionamiento y configuración.*	*Departamento de IT*
Becario	*Reporte*	*Líder del Proyecto*	*Contenido del reporte, así como descripción de las herramientas utilizadas.*	*Líder del Proyecto*
Becario	*Información*	*Líder del Proyecto*	*Links de páginas verídicas con sustento tecnológico.*	*Líder del Proyecto*

2.8 Seguimiento y Control

Los seguimientos para el monitoreo y control por el equipo de trabajo se realizan cada quince días, esto tiene una excepción donde salvo el hito por fecha sea de importancia mayor que en este caso sería semanal. En este punto se discuten los trabajos realizados para determinar las pautas futuras.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

Los principales entregables producidos durante mi estancia en la empresa son:

- Creación de túneles IPSec para asegurar las comunicaciones IP mediante el cifrado y autenticación de cada paquete.
- Reporte de análisis de vulnerabilidades externas.
- Reporte de implementación para el respaldo de información.
- Reporte de auditoría sobre respaldo de usuarios.

3.2 Estimación del Impacto

Haciendo prospección sobre lo que produje puedo decir que el impacto que tiene es importante, ya que le da una idea a la empresa que solicitó el trabajo a la empresa huésped sobre que tan bien o mal están en su infraestructura y que tan grave es si se llega a presentar un fallo o una infiltración no autorizada.

También con la creación de túneles IPSec la compañía puede tener una conexión segura a lo largo del país por sus distintas locaciones, donde se asegura la integridad, confidencialidad y disponibilidad de su información en todo momento. La creación de estos túneles es escalable, por lo que si en cierto momento agregan otro centro se puede agregar la conexión segura en este lugar.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

Las competencias más importantes que desarrollé durante el PAP son:

1. Habilidad de desarrollar reportes técnicos a nivel empresarial validados por especialistas en el tema.
2. Trabajo en equipo como competencia suave.
3. La necesidad de generar consciencia a las empresas de cualquier tamaño sobre la importancia de la implementación de ciberseguridad.
4. Saberes de análisis de vulnerabilidades, interconexión de redes, así como comunicación oral y escrita.

4.2 Aprendizajes Sociales

Aunque mis servicios no contribuyen a beneficios de carácter público, considero que es un beneficio que le brindará seguridad a los empleados y dueños de la empresa que su información no caerá en manos equivocadas en este mundo donde los ataques informáticos se están volviendo más constantes.

Considero que este proyecto ayudará a personas interesadas en el ámbito de la ciberseguridad a adentrarse a las oportunidades que dan este tipo de empresas e impulsarlos a investigar y trabajar en este rubro.

Si cambiaron mi visión del mundo social en las empresas tecnológicas, ya que yo anteriormente pensaba que el ambiente laboral sería que cada uno estaba enfocado en lo suyo y existiría una "competencia" por quien sabe más, pero me di cuenta que es todo lo contrario, siempre hay alguien que está dispuesto a ayudarte y existe un gran ambiente de trabajo.

4.3 Aprendizajes Éticos

Considero que la ética es fundamental para cualquier empleo, pero en especial para la ciberseguridad, sin una base ética no se pudiera desarrollar un análisis de vulnerabilidades de manera óptima y la gente ocultaría ciertos aspectos importantes para su beneficio propio.

Esto me lleva a querer ayudar tanto a las empresas como a las personas de informarse y protegerse de las vulnerabilidades más comunes para que no sean las víctimas de los agresores cibernéticos.

Con esto me queda claro cómo y para quién habré de ejercer mi profesión una vez terminada mi experiencia PAP, esto también gracias por parte a un profesor que nos dijo que vale más nuestra reputación que cualquier cantidad de dinero.

4.4 Aprendizajes Personales

La experiencia de estar en el PAP me dio los elementos que ayudaron a conocer mis habilidades que aplico en la empresa huésped y me ayudó también a reconocer como es el ambiente laboral en una empresa tecnológica enfocada al cien por ciento a la ciberseguridad. Me sirvió para entender que el ámbito de la ciberseguridad es muy amplio y que está bien no saber de todo, pero de lo que sepas debes tener mucho conocimiento.

El haber participado en este proyecto PAP me ayudó proyectar mejor mi proyecto de vida profesional ya que debo de tomar siempre las oportunidades que se me presenten y siempre buscar que es lo mejor para mi y no para la empresa, enfocarme cien por ciento en mi y que es lo que quiero aprender o en donde más quiero tomar experiencia y desarrollarme.

4.5 Tareas Aprendidas

Las acciones y actitudes que tuvo el líder de proyecto ayudaron en gran parte en el éxito de los entregables, ya que, gracias a su gran dominio del tema, nos apoyaba en todo momento en cualquier duda o inquietud que tuviéramos sin importar las veces que lo tuviera que repetir hasta que quedara claro. La comunicación que había dentro del grupo entre el equipo de trabajo fue un factor que también promovía no tener miedo a preguntar y se generó un buen ambiente laboral. También el tener la iniciativa de investigar y aprender conocimientos que no son adquiridos en mi carrera siento que tomó un papel importante en mi desarrollo en este PAP, por lo que ahora tengo las ganas de seguir aprendiendo temas de relevancia en ciberseguridad aún cuando no sean necesarios para usarse en la empresa huésped o en la universidad.

La situación que pudo realizarse de una mejor manera fue que al inicio nos retrasamos un poco porque todavía no empezaba el contrato de la empresa huésped con el cliente que quería de los servicios de ciberseguridad, por lo que estuvimos un par de semanas sin poder desarrollar alguna tarea.

5. Conclusiones

Como conclusión, el haber participado en este proyecto PAP me ayudó mucho en identificar las habilidades que tengo y también en desarrollar habilidades nuevas en el ámbito laboral. También me ayudó a darme cuenta que no todas las personas entienden conceptos de tecnología, por lo que un documento como un reporte les puede ayudar a entender en palabras no técnicas los aspectos que son importante cambiar y las repercusiones que estos pudieran tener.

Una experiencia que tuve fue que en la creación de túneles IPSec me equivoqué en el direccionamiento IP que debía poner, por lo que no había conexión con un centro de datos en un estado de la república. Aunque me angustié, mi líder de proyecto me ayudó a corregir el error el cual no tuvo ningún impacto negativo; pero lo que me gustó fue que no percibí ninguna molestia por parte del líder y estuvo muy dispuesto a que aprendiera como corregir mi error.

Como mencioné anteriormente en este documento, esta bien no saber todo de ciberseguridad por ser una rama amplia de conocimientos, por lo que esta bien siempre pedir ayuda después de haber investigado por tu cuenta y no encontrar respuesta alguna. Porque si se vive con el temor de ser juzgado por no saber cierto tema, está peor después hacer algo de una manera que no fue requerido y haber perdido tiempo en esa realización. Considero que es importante crear un ambiente de confianza entre los compañeros de equipo y ser solidarios para explicar cuando alguien mas desconoce de cierto tema.

Para terminar, me siento muy satisfecho personalmente al haber terminado esta etapa de esta manera. Adquirí conocimiento y experiencia que la universidad no puede dar, pero esto fue gracias también a mi esfuerzo para lograr los objetivos que se me presentaban. Me quedo principalmente con que siempre hay que tener iniciativa por querer saber más e investigar las nuevas tecnologías, esto porque, así como la tecnología avanza, las técnicas de ataques y los grupos criminales también avanzan a pasos agigantados por lo que siempre debemos estar un paso por delante de ellos.

6. Bibliografía y Anexos (*solo en caso de ser necesarios*)

[Son los documentos bibliográficos utilizados para la elaboración del reporte. Debe de utilizarse el sistema APA]

[Es todo lo que soporte el documento; que no es necesario añadirlo en el cuerpo del reporte, pero que sirve para su mejor comprensión: materiales elaborados, bitácoras, fichas, fotografías, mapas, etc.]