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 TECNOLOGIA I

BAXTER

PRESENTA

Alumno: CIB, Emiliano Arroyo Valencia

Profesor PAP: 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

En el contexto actual de transformación digital, la gestión efectiva de la seguridad en la nube se ha convertido en una prioridad para las organizaciones. En Baxter, la administración de la postura de seguridad en la nube (CSPM, por sus siglas en inglés: Cloud Security Posture Management) es fundamental para mitigar riesgos y garantizar el cumplimiento normativo. Las herramientas de CSPM automatizan la detección de errores de configuración en los recursos de la nube, permitiendo a las organizaciones reducir la probabilidad de infracciones y mejorar su postura de seguridad.

Actualmente, Baxter cuenta con múltiples herramientas dedicadas a la seguridad en la nube. Sin embargo, se ha identificado que, aunque estas herramientas son capaces de detectar errores de configuración, no siempre se reportan de manera efectiva a los responsables de los recursos afectados. Esta falta de comunicación ha llevado a que algunas vulnerabilidades permanezcan sin ser atendidas, incrementando potencialmente el riesgo para la organización.

Ante esta problemática, mi contribución se centró en optimizar el proceso de reporte y gestión de estas detecciones. Para ello, realicé un análisis exhaustivo del estado actual de las herramientas CSPM utilizadas, identificando áreas de mejora y oportunidades de optimización. Posteriormente, elaboré una propuesta detallada para mejorar la gestión de alertas, basándome en las mejores prácticas de seguridad y en la integración con otras herramientas de ciberseguridad ya implementadas en la empresa. Este enfoque busca no solo automatizar la generación y envío de reportes a los responsables correspondientes, sino también establecer un procedimiento claro para la gestión y escalamiento de alertas dentro del equipo de seguridad en la nube.

La implementación de estas mejoras tiene como objetivo fortalecer la postura de seguridad de Baxter, garantizando una respuesta más ágil y efectiva ante posibles vulnerabilidades en su infraestructura en la nube.

1. Introducción

Durante el desarrollo de este PAP, llevaré a cabo una mejora en los procesos de seguridad en la nube dentro del área de Cloud Security de Baxter, una empresa global enfocada en el desarrollo de equipamiento médico. Este proyecto se enfocará en optimizar la administración de la postura de seguridad en la nube (CSPM, por sus siglas en inglés), asegurando una mejor gestión y reporte de alertas relacionadas con configuraciones de seguridad en los entornos cloud de la empresa.

El objetivo principal será mejorar el flujo de notificación de errores detectados por las herramientas de CSPM, garantizando que los responsables de cada recurso en la nube reciban información precisa y oportuna para la mitigación de riesgos. Actualmente, Baxter cuenta con múltiples herramientas dedicadas a este rubro, sin embargo, no se les ha dado el seguimiento adecuado, lo que ha generado un vacío en la resolución de alertas de configuración.

Como parte del proyecto, exploraré estrategias para la integración de estas herramientas con otros sistemas de ciberseguridad de la empresa, permitiendo un monitoreo más eficiente y una respuesta más ágil ante posibles vulnerabilidades. Esto requerirá análisis, diseño y pruebas de soluciones que optimicen los procesos internos del área de Cloud Security.

El desarrollo de este PAP representará una oportunidad para aplicar mis conocimientos adquiridos en la Ingeniería en Ciberseguridad, fortaleciendo habilidades en la gestión de seguridad en la nube y el uso de herramientas avanzadas en el sector. A lo largo del proyecto, colaboraré con distintos equipos dentro de la organización, permitiendo una visión integral de las operaciones de seguridad en entornos cloud.

Este proyecto lo desarrollaré dentro del marco de tiempo establecido por la empresa y la Coordinación PAP-DESI, considerando las necesidades del área y las expectativas de mejora en la postura de seguridad en la nube. Al finalizar, se espera haber implementado soluciones que permitan una administración más eficiente de los riesgos en los entornos cloud de Baxter, mejorando la seguridad y cumplimiento normativo de la organización.

1.1 Antecedentes

La organización huésped es Baxter, una empresa estadounidense con sede en Deerfield, Illinois. Se especializa en el desarrollo de equipamiento médico y se enfoca en diversas ramas tecnológicas orientadas al cuidado de la salud. Entre sus productos se destacan soluciones intravenosas, camas de hospital y dispositivos clave para el

tratamiento, como sistemas de diálisis, que son fundamentales para el sector sanitario.

Baxter atiende a hospitales, clínicas de diálisis y otras instituciones de salud, consolidándose como un referente en la provisión de tecnología médica de alta calidad. Su presencia es global, operando en más de 100 países, lo que le permite satisfacer las necesidades de un amplio espectro de clientes en diversos mercados internacionales.

La misión que inspira a Baxter es "salvar y sostener vidas". Este enfoque ético y profesional respalda su trayectoria y la posiciona como un aliado estratégico para la mejora continua en la atención médica a nivel mundial.

1.2 Justificación

Mi motivación para invertir mi esfuerzo en este PAP surge de la oportunidad de integrar y aplicar los conocimientos adquiridos en la Ingeniería en Ciberseguridad en un entorno real y de alta exigencia como lo es Baxter. La experiencia me permitirá relacionar la teoría aprendida en áreas como análisis de riesgos, administración de sistemas de seguridad y auditorías de configuración con las prácticas y desafíos que se presentan en el ámbito profesional, fortaleciendo mi perfil técnico y profesional.

Estimo dedicar aproximadamente 25 a 30 horas semanales a este proyecto, tiempo que incluye tanto la ejecución de las actividades asignadas como la capacitación continua para adquirir competencias específicas relacionadas con las necesidades de la empresa.

Para el desarrollo exitoso de este PAP cuento con diversos apoyos y recursos ofrecidos por Baxter y el ITESO, entre los cuales destacan:

- La supervisión y mentoría directa por parte de un experto en ciberseguridad en Baxter.
- Acceso a herramientas y plataformas tecnológicas de última generación que facilitan la práctica y el análisis en entornos reales.
- Capacitaciones y talleres internos que fortalecen las competencias técnicas y operativas.
- Apoyo económico por parte de Baxter para certificarme en áreas requeridas para mis tareas dentro de la empresa.

Finalmente, considero que esta línea de negocio es sumamente atractiva para mi desarrollo profesional, ya que me brinda la oportunidad de especializarme en áreas

críticas de la ciberseguridad como lo es el sector de la salud, abriendo puertas a futuras oportunidades en el sector al culminar mi carrera.

1.3 Objetivos

Baxter realiza proyectos PAP con el fin de impulsar la innovación y mejorar sus procesos internos, en particular en áreas críticas de la tecnología, pues las instalaciones de Guadalajara, junto con las instalaciones en la India, son los dos únicos centros globales de tecnologías de la información de Baxter.

A través de estos proyectos, la empresa busca incorporar soluciones tecnológicas frescas a través de los estudiantes. Además, al colaborar con instituciones académicas, Baxter fortalece el vínculo con la comunidad educativa, aprovechando el talento joven para enriquecer su capacidad de adaptación y respuesta ante los desafíos del mercado global.

Durante mi participación en este PAP, aspiro a profundizar en el conocimiento práctico de las tecnologías de ciberseguridad, enfocándome en el uso y experimentación con herramientas de seguridad. Mi objetivo es aplicar y ampliar los conocimientos adquiridos en el ITESO, desarrollando competencias que me permitan identificar, analizar y solucionar problemas en entornos reales de alta complejidad. Asimismo, espero fortalecer mis habilidades en gestión de proyectos, trabajo colaborativo y comunicación técnica, lo que contribuirá a mi formación integral y me preparará para futuros desafíos profesionales en el ámbito de la ciberseguridad.

1.4 Contexto

El PAP en el que participo se desarrolla dentro del área de Cloud Security de Baxter, la cual se encarga de garantizar la seguridad de los recursos en la nube de la empresa. Este departamento tiene como objetivo la protección de la infraestructura y los datos almacenados en entornos cloud, asegurando el cumplimiento de normativas y buenas prácticas de ciberseguridad.

El tipo de proyecto en el que participo se enfoca en la mejora de procesos, específicamente en la optimización del reporte de detecciones realizadas por las herramientas de CyberSecurity Postura Management (CSPM). Actualmente, aunque estas herramientas identifican errores de configuración en la nube, no se les da un seguimiento adecuado, lo que impide la resolución de los problemas detectados.

Mi rol dentro del proyecto es el de Intern, y mis funciones incluyen el análisis del flujo actual de reportes de seguridad en la nube, la identificación de áreas de mejora en la gestión de alertas y la exploración de posibles integraciones con otras herramientas

de ciberseguridad utilizadas en la empresa. A lo largo de mi participación, colaboraré con el equipo de Cloud Security para diseñar y proponer soluciones que optimicen estos procesos, contribuyendo así a una administración más eficiente y segura de la infraestructura cloud de Baxter.

1.5 Inventario de Competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	**Uso de herramientas para la seguridad en la nube**	3	1	2	3	M
1.1	Uso y monitoreo de Cloudflare para seguridad WAF	3	1	2	3	M
1.2	Monitoreo y reporte de alertas de seguridad en PrismaCloud	3	1	2	3	M
1.3	Capacitación en el uso y monitoreo de Crowdstrike Cloud	3	1	2	3	A
2	**Programación en Python**	1	2	0	1	A
2.1	Scripting para crear herramientas	1	2	0	1	M
2.2	Automatizar tareas cotidianas	1	2	0	1	A
3	**Inglés Conversacional**	3	2	1	3	M
3.1	Envío de reportes en inglés por correo	3	2	1	3	M
3.2	Llamadas en inglés con el resto del equipo fuera de México	3	2	1	3	A
4	**Reporte de alertas de seguridad**	3	1	2	3	M
4.1	Envío de correos notificando vulnerabilidades a los encargados de activos	3	1	2	3	M
4.2	Reportes de estatus de alertas enviadas	3	1	2	3	M
5	**Identificación de amenazas informáticas en tendencia**	1	1	2	1	A
5.1	Creación y presentación de diapositivas informando nuevas tendencias	1	1	0	1	A
5.2	Envío por correo de nuevas tendencias	1	1	0	1	A

1.6 Plan Educativo

No.	Actividad Educativa	Tipo Actividad	Total Hrs	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	9	10	Obj
1	**Uso de herramientas para la seguridad en la nube**															
1.1	Aprendizaje y conocimiento de CloudFlare para seguridad WAF	Tutoría	4	17 de marzo	26 de marzo											
1.2	Aprendizaje y conocimiento de PrismaCloud	Tutoría	6	27 de enero	12 de febrero											
1.3	Aprendizaje y conocimiento de Crowdstrike Cloud	Tutoría	4	17 de febrero	26 de febrero											
2	**Programación en Python**															
2.1	Conocer librerias y codigo para crear herramientas	Autoestudio	2	24 de febrero	28 de febrero											
2.2	Conocer cuando si y cuando no automatizar una tarea	Tutoría	2	24 de febrero	28 de febrero											
3	**Inglés Conversacional**															
3.1	Practicar el idioma en el nivel técnico necesario.	Autoestudio	4	27 de enero	7 de febrero											
3.2	Mejorar la comunicación con expresiones nativas.	Autoestudio	4	27 de enero	7 de febrero											
4	**Reporte de alertas de seguridad**															
4.1	Creación de formato para los reportes a enviar.	Practica	2	17 de febrero	17 de febrero											
4.2	Conocer las principales vulnerabilidades que afectan a los activos.	Tutoría	6	24 de febrero	14 de marzo											
5	**Identificación de amenazas informaticas en tendencia**															
5.1	Configuración de fuentes confiables al panel de noticias	Practica	1	10 de marzo	10 de marzo											
5.2	Desarrollo de habilidades comunicativas con perfiles no tecnicos	Practica	2	10 de marzo	14 de marzo											

1.7 Entregables

- Análisis del estado actual de la herramienta CSPM: Documento que describe el flujo actual de detección y reporte de errores de configuración en la nube, identificando áreas de mejora y oportunidades de optimización.

- Propuesta de mejora en la gestión de alertas: Informe detallado con recomendaciones para optimizar la detección, el seguimiento y la notificación de errores de configuración en los recursos cloud, con base en mejores prácticas de seguridad.

- Implementación o configuración de integraciones: En caso de ser viable, documentación sobre la integración de herramientas de ciberseguridad que permitan automatizar la generación y envío de reportes a los responsables de los recursos afectados.

- Guía de uso o procedimiento actualizado: Documento con instrucciones para la correcta gestión y escalamiento de alertas dentro del equipo de seguridad en la nube.

1.8 Involucrados

Los principales actores interesados en los resultados del proyecto PAP incluyen:

- Área de Cloud Security: Responsable de la seguridad de los recursos en la nube de la empresa. Es el área solicitante del proyecto y la principal beneficiaria de las mejoras en la gestión de alertas de configuración.

- Gerente encargado PAP: Mi supervisor encargado de guiar y evaluar el desarrollo del proyecto, asegurando que las mejoras propuestas se alineen con los objetivos de la empresa y las mejores prácticas de seguridad.

- Equipos de Infraestructura: Áreas que gestionan y operan los recursos en la nube, y que recibirán los reportes optimizados sobre errores de configuración para su corrección.

- Área de Cumplimiento y Auditoría: Departamento interesado en mejorar la visibilidad y trazabilidad de los incidentes de seguridad para cumplir con normativas y regulaciones.

- Intern: Yo, encargado de analizar, proponer e implementar mejoras en el flujo de detección y notificación de alertas en la nube, colaborando con los distintos equipos involucrados.

El éxito del proyecto impactará directamente en la seguridad y cumplimiento normativo de los recursos cloud de la empresa, mejorando la eficiencia en la identificación y corrección de vulnerabilidades.

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

En la fase de Inicio, defino los objetivos y el alcance del proyecto, recopilando la información necesaria para establecer las bases del PAP. Establezco los entregables y obtengo la aprobación de mi líder técnico en Baxter, asegurando que se comprendan las metas y expectativas del proyecto.

Durante la Planificación, desarrollo un cronograma detallado en el que asigno tareas, recursos y tiempos específicos para cada actividad. Elaboro un plan que contempla tanto las acciones técnicas como las capacitaciones necesarias, coordinando con el equipo de Cloud Security para asegurar la viabilidad y coherencia de las acciones propuestas.

En la etapa de Ejecución, implemento las actividades planificadas, realizando análisis, pruebas y ajustes en el sistema de reporte de alertas. Mantengo una comunicación constante con los miembros del equipo, garantizando que cada tarea se desarrolle de acuerdo con el plan establecido.

Para el Seguimiento y Control, monitoreo de forma continua el progreso del proyecto a través de indicadores de rendimiento y reuniones periódicas. Reviso y ajusto el plan según sea necesario, verificando el cumplimiento de los objetivos y la calidad de los entregables.

Finalmente, en la fase de Cierre, recopilo y documento los resultados obtenidos, elaborando un informe final que sintetiza las mejoras implementadas, los aprendizajes y las recomendaciones para futuros proyectos.

2.2 Sustento Teórico y Metodológico

No se emplea un proceso formal basado en metodologías ágiles, dado que el equipo es pequeño y se adapta a procedimientos internos propios de Baxter. La coordinación y comunicación se realizan de manera informal pero estructurada, mediante el uso de Microsoft Teams y correo electrónico, lo que permite mantener un registro detallado de las decisiones y acciones implementadas. Además, se utilizan varias carpetas compartidas para centralizar y actualizar de forma continua la documentación y archivos relevantes del proyecto.

Esta aproximación flexible facilita la adaptación a las necesidades del proyecto y garantiza la calidad en la producción de los entregables, sin recurrir a marcos metodológicos rígidos.

2.3 Descripción del Proyecto

El proyecto PAP que desarrollo en Baxter se centra en la optimización del proceso de reporte de errores de configuración detectados por las herramientas de CSPM en el área de Cloud Security. Conforme al plan de trabajo establecido, se identifican y analizan las etapas actuales de detección y notificación, generando sub-entregables que incluyen análisis del flujo de información, propuestas de mejora y, de ser viable, la integración de soluciones para automatizar el reporte de alertas.

El proyecto se desarrolla siguiendo un ciclo de vida iterativo, lo que permite evaluar y ajustar continuamente las propuestas en función de la retroalimentación obtenida. Aunque este proyecto se presenta como un módulo independiente enfocado en la mejora de procesos de seguridad en la nube, se integra dentro del conjunto de iniciativas de Baxter destinadas a optimizar la administración de riesgos en entornos digitales.

Recursos Tecnológicos y Herramientas

Entre los recursos más importantes que utilizo se encuentran:

- Plataformas de comunicación y gestión documental: Uso de Microsoft Teams, Outlook y carpetas compartidas para coordinar el trabajo en equipo y mantener un registro actualizado de la información y decisiones.
- Sistemas y herramientas de CSPM: Empleo de las soluciones de seguridad ya implementadas en la empresa para la detección y análisis de errores en la configuración de recursos en la nube. Algunos ejemplos son: PrismaCloud, Crowdstrike Cloud, Salt, Cloudflare, etc.
- Software de análisis y documentación: Herramientas de análisis de datos y elaboración de informes como Word o Excel que facilitan la integración y presentación de las propuestas de mejora al resto del equipo.

2.4 Plan de Trabajo

No.	Actividad Educativa	Encargado	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	**Uso de herramientas para la seguridad en la nube**																			
1.1	Aprendizaje y conocimiento de CloudFlare para seguridad WAF	Alex (líder PAP) y Kumar	17 de marzo	26 de marzo																
1.2	Aprendizaje y conocimiento de PrismaCloud y SALT	Alex (líder PAP)	27 de enero	12 de febrero																
1.3	Aprendizaje y conocimiento de Crowdstrike Cloud	Alex (líder PAP)	17 de febrero	26 de febrero																
2	**Programación en Python**																			
2.1	Creacion de script para recolectar registros DNS de todo Baxter	Yo	31 de marzo	25 de abril																
2.2	Creacion de script para automatización de envio de alertas	Alex (líder PAP)	24 de febrero	25 de abril																
3	**Inglés Conversacional**																			
3.1	Reporte de actividades realizadas por la semana	Yo	27 de enero	9 de mayo																
3.2	Redacción de plantillas para envio de alertas	Yo	27 de enero	24 de marzo																
4	**Reporte de alertas de seguridad**																			
4.1	Reporte de alertas de SALT	Alex (líder PAP)	31 de marzo	9 de mayo																
4.2	Reporte de alertas de PrismaCloud	Alex (líder PAP)	10 de febrero	24 de marzo																
5	**Identificación de amenazas informaticas en tendencia**																			
5.1	Busqueda de tendencias y creacion de presentación	Ellen	17 de febrero	2 de mayo																
5.2	Comunicar con perfiles no tecnicos	Ellen y Jeff	24 de febrero	9 de mayo																

2.5 Equipo de Trabajo

Rol	*Responsabilidad*	*Nombre (opcional)*
Consultor Cloud Security (Mi líder técnico)	Administra las herramientas de la administración de la postura de ciberseguridad y el WAF de Cloudflare, gestionando las reglas de seguridad que mantienen a los sitios web de Baxter seguro de atacantes externos.	Alex
Becario Cloud Security	Apoyar en la ejecución de herramientas de ciberseguridad, de alguna forma pivoteamos entre todas las responsabilidades del equipo, ya sea generando reportes, contactando gente o realizando ajustes menores a las herramientas que usamos o recolectando nuevas tendencias de ciber amenazas,	Abraham
Becario Cloud Security	Apoyar en la ejecución de herramientas de ciberseguridad, de alguna forma pivoteamos entre todas las responsabilidades del equipo, ya sea generando reportes, contactando gente o realizando ajustes menores a las herramientas que usamos o recolectando nuevas tendencias de ciber amenazas,	Josué
Becario Cloud Security	Apoyar en la ejecución de herramientas de ciberseguridad, de alguna forma pivoteamos entre todas las responsabilidades del equipo, ya sea generando reportes, contactando gente o realizando ajustes menores a las herramientas que usamos o recolectando nuevas tendencias de ciber amenazas,	Emiliano (yo)
Consultor Threat Intelligence	Monitorea amenazas cibernéticas en tendencia e investiga noticias relevantes sobre ciberataques, recolecta toda esta información y la facilita a los cargos administrativos para la toma de decisiones.	Ellen
Consultor Cloudflare	Administra y monitorea la herramienta Cloudflare, gestionando los registros DNS, de todos los sitios en Baxter junto con su WAF y algunas otras características de la herramienta.	Kumar
Director Cloud Security	Se encarga de mostrar periódicamente todos los resultados de nuestro equipo al área administrativa y cargos más altos.	Jeff

2.6 Plan de Comunicaciones

Emisor	*Mensaje*	*Receptor*	*Medio*	*Frecuencia*
Consultor Cloud Security (Alex)	Informe de avances, y actualizaciones de tareas	Becarios Cloud Security (Abraham, Josué, Emiliano)	Email, Teams, juntas virtuales	Semanal (s)
Becarios Cloud Security	Reporte de actividades y hallazgos en el reporte de alertas de CSPM	Consultor Cloud Security (Alex	Email, carpeta compartida, Teams	Semanal (s)
Consultor Threat Intelligence (Ellen) y Becarios Cloud Security	Información sobre tendencias y amenazas cibernéticas	Director Cloud Security (Jeff) y equipo de ciberseguridad	Reuniones virtuales	Bisemanal (2s)
Consultor Cloudflare (Kumar)	Actualización de registros DNS y configuraciones del WAF	Equipo técnico encargado del sitio web y Alex	Email	Bimestral (2m)
Director Cloud Security (Jeff)	Reporte de resultados y estrategias generales	Área Administrativa y equipo de seguridad	Presentaciones, email, reuniones	Semanal (s)
Becario Cloud Security (Emiliano)	Avances del proyecto y consultas específicas sobre tareas	Profesor PAP	Canvas, junta virtual	Mensual (m)

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.*
Becarios Cloud Security	Análisis del estado actual de la herramienta CSPM: Documento que describe el flujo actual de detección y reporte, identificando áreas de mejora.	Consultor Cloud Security (Alex)	Documento completo, claro y preciso; identificación adecuada de errores y oportunidades de optimización; alineación con los estándares de seguridad.	Retroalimentación y aprobación para avanzar a la elaboración de la propuesta.

Becarios Cloud Security	Propuesta de mejora en la gestión de alertas: Informe detallado con recomendaciones para optimizar la detección, seguimiento y notificación de errores.	Consultor Cloud Security (Alex)	Propuesta fundamentada en mejores prácticas; factibilidad técnica; coherencia con el análisis previo; claridad en las recomendaciones y procesos de integración propuestos.	Revisión adicional por el Director Cloud Security (Jeff) y ajustes en la propuesta.
Becarios Cloud Security	Implementación o configuración de integraciones: Documentación sobre la integración de herramientas para automatizar el reporte.	Consultor Cloud Security (Alex) y equipo cloud security	Documentación detallada que demuestre la integración efectiva; viabilidad técnica comprobada; compatibilidad con la infraestructura actual; cumplimiento de requisitos de seguridad.	Pruebas de integración y validación final en el entorno productivo.
Becarios Cloud Security	Guía de uso o procedimiento actualizado: Documento con instrucciones claras para la gestión y escalamiento de alertas en el equipo.	Consultor Cloud Security (Alex)	Instrucciones precisas y comprensibles; procedimiento probado y validado; consistencia con los procesos internos; feedback positivo de usuarios clave.	Distribución y capacitación interna sobre el nuevo procedimiento.

2.8 Seguimiento y Control

El monitoreo y control del proyecto se lleva a cabo a través de una estructura flexible pero organizada, alineada con los procedimientos internos de Baxter. Dado que no se sigue una metodología ágil formal, el seguimiento se realiza mediante reuniones periódicas y el uso de herramientas colaborativas para documentar avances, identificar obstáculos y tomar acciones correctivas cuando sea necesario.

Seguimiento interno con el equipo de trabajo

El equipo de trabajo, liderado por el Consultor Cloud Security (Alex), realiza reuniones de seguimiento con los becarios de Cloud Security (Abraham, Josué y Emiliano) con la siguiente periodicidad y objetivos:

- Reuniones semanales (Teams o presenciales según disponibilidad):
    - Revisión de avances en los entregables.
    - Identificación de bloqueos o problemas técnicos.
    - Evaluación del cumplimiento de fechas programadas.
    - Ajustes en la asignación de tareas si es necesario.
- Reportes de progreso en carpetas compartidas (continuo):
    - Actualización de documentos y hallazgos en tiempo real.
    - Revisión y retroalimentación de avances en tareas.
- Correos electrónicos para ajustes puntuales (según necesidad):
    - Comunicación de cambios en el plan de trabajo.
    - Priorización de tareas urgentes o imprevistos.
    - Coordinación con otros equipos en caso de requerir apoyo externo.

En caso de retrasos en los entregables, se documentan las causas y se implementan acciones correctivas, como la redistribución de tareas, la reasignación de plazos o la búsqueda de soluciones técnicas alternativas.

Seguimiento con la Coordinación PAP y el Profesor PAP

Para garantizar el alineamiento con los objetivos del Proyecto PAP, se llevan a cabo interacciones regulares con la Coordinación PAP y el Profesor PAP, a través de:

- Juntas mensuales de revisión con el Profesor PAP:
    - Presentación de avances y ajustes en el reporte.
    - Revisión de cumplimiento de objetivos y posibles desviaciones.
    - Asignación de nuevas responsabilidades si es necesario.
- Eventos programados con la Coordinación PAP:
    - Evaluaciones parciales y retroalimentación sobre el desarrollo del proyecto.
    - Validación del Reporte Final PAP y sugerencias de mejora.
    - Coordinación de entregables finales y cierre del proyecto.

Esta estructura de seguimiento permite mantener un control efectivo del proyecto, garantizando que los entregables sean desarrollados conforme a los estándares de calidad esperados y en alineación con los objetivos del Proyecto PAP.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

Durante mi participación en el PAP, he desarrollado varios entregables que ya están demostrando su valor en la organización y que se proyectan como herramientas clave para el futuro. Los principales productos obtenidos son:

1. Análisis del estado actual de la herramienta CSPM:
   Este documento describe de forma detallada el flujo actual de detección y reporte de errores de configuración en la nube, identificando áreas de mejora y oportunidades de optimización. Durante su elaboración, nos enfrentamos a desafíos en la integración de datos provenientes de diversas fuentes, lo que fortaleció mi capacidad de análisis y resolución de problemas.

2. Propuesta de mejora en la gestión de alertas:
   Elaboré un informe con recomendaciones basadas en las mejores prácticas de seguridad, orientado a optimizar la detección, seguimiento y notificación de errores. Aunque fue necesario ajustar las propuestas para alinearlas con las limitaciones técnicas existentes, este proceso me permitió aprender a adaptar soluciones teóricas a un entorno real.

3. Implementación o configuración de integraciones:
   Se generó una serie de automatizaciones y una documentación que detalla la integración de herramientas de ciberseguridad para automatizar la generación y envío de reportes a los responsables de los recursos afectados. Este entregable, resultado de múltiples iteraciones y pruebas, ha sido fundamental para validar la viabilidad técnica de las integraciones propuestas, enfrentando y superando desafíos en la interconexión de sistemas.

4. Guía de uso o procedimiento actualizado:
   Este producto se encuentra en proceso de creación y perfeccionamiento. Su objetivo es proporcionar instrucciones claras para la gestión de las nuevas integraciones automatizadas dentro del equipo de seguridad en la nube, y continuará evolucionando a medida que se recoja retroalimentación y se ajusten los procesos a la práctica diaria.

3.2 Estimación del Impacto

El análisis de los entregables desarrollados me revela un impacto significativo tanto para Baxter como para sus clientes y la comunidad en general. Los entregables aportan una base sólida para identificar y corregir deficiencias en la detección y reporte de errores de configuración en la nube, no solo en la herramienta que ya usamos, también se puede replicar en las herramientas venideras y así reducir el margen de error y el juicio humano al momento de reportar alertas. Esto se traduce en una mayor eficiencia operativa y en una reducción del riesgo de vulnerabilidades, beneficiando directamente a Baxter en su objetivo de mantener altos estándares de ciberseguridad.

Aunque la Guía de uso o procedimiento actualizado aún se encuentra en proceso de perfeccionamiento, su desarrollo apunta a establecer un protocolo claro y replicable que facilite la capacitación del personal y asegure la continuidad en la gestión de alertas. Esto impactará positivamente en la consistencia y calidad de las operaciones diarias.

En conjunto, estos productos no solo fortalecen la infraestructura de seguridad de la organización, sino que también promueven una cultura de mejora continua y aprendizaje colaborativo. La optimización de estos procesos se traduce en beneficios tangibles, como la reducción de incidentes y una mayor capacidad de respuesta ante amenazas, lo que a su vez eleva la confianza de clientes y usuarios en los servicios de Baxter.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

He desarrollado diversas competencias que se han consolidado tanto a nivel técnico como en habilidades interpersonales y de gestión:

- Competencias técnicas y profesionales:
  He profundizado mi conocimiento en infraestructura cloud, no solo mejorando mi capacidad para detectar y reportar errores de configuración, también he aprendido un poco de arquitectura de AWS. Esto me ha permitido aplicar conceptos de gestión de riesgos, integración de sistemas de ciberseguridad y análisis de datos, alineados con las mejores prácticas de la industria. Además, he fortalecido mi habilidad para elaborar propuestas técnicas y documentar soluciones, temas muy importantes que no se suelen tocar en mi formación en ciberseguridad.

- Competencias suaves y de gestión:
  La experiencia me ha impulsado a mejorar mi comunicación efectiva, tanto en la coordinación con el equipo de Cloud Security como en la interacción con mentores y otros colaboradores. También he desarrollado habilidades de liderazgo y trabajo en equipo, esenciales para identificar problemas, proponer soluciones y tomar decisiones en un entorno dinámico y multidisciplinario.

- Aprendizajes sobre el contexto sociopolítico y económico:
  He comprendido la relevancia de la ciberseguridad en sectores críticos, como el de la salud, y su impacto en la estabilidad operativa de organizaciones globales. Este entendimiento me permite apreciar cómo factores económicos y políticos influyen en la implementación de estrategias de seguridad, y la importancia de adaptar soluciones a contextos específicos.

- Aplicación de saberes universitarios:
  Los fundamentos teóricos y prácticos adquiridos en la carrera han sido puestos a prueba al enfrentar desafíos reales, permitiéndome trasladar conocimientos sobre todo de cloud, normativas de seguridad y análisis de sistemas a situaciones del entorno laboral, en ITESO solo llevamos una materia sobre cloud, pero aun así fue un gran apoyo para lograr certificarme en la nube de AWS.

4.2 Aprendizajes Sociales

El proyecto PAP ha contribuido a la sociedad al reforzar la seguridad de infraestructuras críticas en el sector salud, lo que se traduce en una mayor protección de datos sensibles y, en consecuencia, en un servicio de atención médica más confiable y seguro. Este esfuerzo de optimización en la gestión de alertas en la nube no solo fortalece la operatividad interna de la empresa, sino que tiene un impacto directo en la calidad de vida de pacientes y profesionales de la salud, quienes dependen de sistemas robustos y resilientes para ofrecer cuidados de calidad.

He aprendido que la innovación en ciberseguridad puede generar prácticas sociales transformadoras. Por ejemplo, la integración de herramientas automatizadas para el reporte puede ser replicada en otros sectores públicos, ampliando el acceso a soluciones de seguridad sin requerir grandes inversiones. De esta manera, se benefician especialmente grupos que tradicionalmente cuentan con recursos limitados para implementar medidas de protección.

4.3 Aprendizajes Éticos

Durante mi experiencia en el PAP, mis valores personales de integridad y responsabilidad se vieron reflejados en cada decisión que tomé. Encontré una profunda concordancia entre mi compromiso ético y el sentido social de Baxter, cuya misión de "salvar y sostener vidas" resuena con mi propia convicción de contribuir a un bien mayor. En varias ocasiones, me enfrenté a dilemas éticos que requerían actuar con transparencia y firmeza, especialmente al reportar vulnerabilidades que, de no ser atendidas, podrían haber comprometido la seguridad de información sensible.

Una situación particular me invitó a tomar una decisión bajo un contexto de incertidumbre: detecté una anomalía que, aunque no era inminente, podía representar un riesgo potencial para la confidencialidad de datos en el entorno cloud, pero el encargado de ese entorno nunca contestaba a nuestros reportes de alertas, por un momento pensábamos en dejar de reportarle porque solo nos desgastábamos, pero por ética decidimos reportar de inmediato esta situación a un compañero de su equipo encargado, a pesar de que el propio encargado nos ignoraba, su compañero tuvo la disposición suficiente para buscar una solución. El nosotros realizar está acción, validada posteriormente por mi mentor, reafirmó mi convicción de que mi profesión no solo se trata de aplicar conocimientos técnicos, sino también de ejercer un profundo compromiso social.

4.4 Aprendizajes Personales

Esta experiencia en el PAP me ha permitido un crecimiento profundo a nivel personal. He descubierto aspectos de mi personalidad y habilidades que desconocía, confirmando mi vocación y capacidad para enfrentar desafíos reales en el ámbito de la ciberseguridad. Al trabajar en un entorno tan diverso, aprendí a valorar y aprovechar la pluralidad de ideas, lo que me ayudó a reconocer que la diversidad no solo enriquece el trabajo en equipo, sino que también es fundamental para abordar problemas complejos desde distintas perspectivas.

Además, el PAP me abrió los ojos a la importancia de la interconexión entre la tecnología y el bienestar social. Comprender cómo las soluciones de ciberseguridad pueden repercutir en la calidad de vida de las personas me impulsó a asumir un compromiso ético y responsable, extendiendo mi visión más allá de lo técnico para involucrarme en proyectos que generen un impacto positivo en la comunidad.

4.5 Tareas Aprendidas

He podido identificar varios factores y situaciones que han marcado tanto los éxitos como las áreas de oportunidad, lo que me ayudará a crecer profesional y personalmente.

a. Factores, acciones y actitudes favorables

- Compromiso y Colaboración: La dedicación del equipo, junto con la disposición para compartir conocimientos, fue crucial. La comunicación constante y el uso de herramientas colaborativas permitieron un flujo de trabajo ágil y transparente.
- Liderazgo: La guía y el apoyo de nuestro líder técnico fueron fundamentales. Su actitud proactiva y su enfoque en encontrar soluciones nos motivaron a enfrentar los desafíos con determinación.
- Flexibilidad y Adaptabilidad: La capacidad de adaptarse rápidamente a cambios y resolver imprevistos permitió que, a pesar de las dificultades, mantuviéramos el rumbo hacia nuestros objetivos.
- Claridad en Roles y Responsabilidades: La definición precisa de tareas ayudó a que cada miembro supiera exactamente cómo contribuir, lo que facilitó la consecución de los entregables.

b. Situaciones y acciones a mejorar

- Coordinación en Tiempo Real: En ocasiones, la respuesta ante imprevistos fue más lenta de lo deseado. Una coordinación más ágil, quizás mediante reuniones

breves adicionales en momentos críticos, podría haber acelerado la toma de decisiones.

- Retroalimentación Oportuna: Hubo momentos en que la retroalimentación sobre ciertos sub-entregables llegó con retraso, afectando el tiempo destinado a hacer ajustes necesarios.
- Documentación Detallada: Mejorar la documentación de cada proceso no solo facilitaría la replicación en futuros proyectos, sino también el aprendizaje colectivo del equipo.

5. Conclusiones

Participar en este PAP ha sido una experiencia transformadora que va más allá de lo técnico. Durante el desarrollo del proyecto, enfrenté situaciones inesperadas, como la necesidad de resolver rápidamente una falla en la comunicación entre sistemas, lo cual me obligó a pensar de forma creativa y a colaborar estrechamente con mi equipo. Estas experiencias me enseñaron que, en entornos reales, la adaptabilidad y la resiliencia son tan cruciales como los conocimientos técnicos.

A lo largo de este proceso, pude constatar el valor del trabajo en equipo y la importancia de una comunicación fluida. Aprendí a gestionar no solo los aspectos operativos, sino también a equilibrar la presión de cumplir plazos y mantener altos estándares de calidad, lo que me ha preparado para futuros desafíos profesionales y personales.

Asimismo, reflexiono sobre cómo este proyecto ha reforzado mi compromiso ético y mi sentido de responsabilidad hacia el bienestar colectivo. Saber que nuestras propuestas y mejoras pueden contribuir a la seguridad de infraestructuras críticas, en el caso de la salud, me llena de satisfacción y me impulsa a seguir creciendo.

La transición de estudiante a profesional en una empresa real ha sido un viaje lleno de aprendizajes y desafíos. Al principio, me encontré navegando por un entorno donde las expectativas y responsabilidades superaban las experiencias académicas previas. La teoría aprendida en la universidad sentó una base sólida, pero enfrentarse a situaciones reales, con plazos ajustados y consecuencias tangibles, reveló la importancia de habilidades como la adaptabilidad y la toma de decisiones bajo presión.

Una de las lecciones más valiosas fue comprender que el aprendizaje es continuo. En el ámbito de la ciberseguridad, las amenazas evolucionan constantemente, lo que exige una actualización permanente de conocimientos y técnicas. Esta realidad me llevó a buscar certificaciones adicionales y a participar en comunidades profesionales para mantenerme al día con las tendencias y mejores prácticas del sector.

En definitiva, este PAP ha representado un reto significativo, en el que el esfuerzo invertido se vio recompensado tanto en resultados tangibles como en valiosas lecciones de vida. Siento una profunda satisfacción por haber superado las adversidades y por haber emergido con una visión más amplia y humana de mi profesión. Esta experiencia me motiva a continuar innovando y a comprometerme con proyectos que generen un impacto positivo en la sociedad.