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

PAPN01B - PAP PROGRAMA DE LA INDUSTRIA DE ALTA TECNOLOGIA II

BAXTER.

PRESENTA

Alumno: CIB, Emiliano Arroyo Valencia

Profesor PAP: Act. Juan Manuel Islas Espinoza, PMP®

Tlaquepaque, Jalisco, julio 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 este segundo Proyecto de Aplicación Profesional, continúo la línea de trabajo iniciada en el PAP 1, ampliando y consolidando las mejoras en la seguridad de la nube de Baxter.

Mientras que la primera fase se centró en diagnosticar y proponer optimizaciones al proceso de reporte de errores de configuración mediante herramientas CSPM, en este nuevo periodo mi objetivo es implementar y operacionalizar esas recomendaciones, así como integrar nuevas capacidades de detección y respuesta ante incidentes.

Para ello, el alcance de este documento abarca:

1. Implementación de mejoras operativas

   A partir del análisis previo, he puesto en marcha ajustes en Salt para garantizar un monitoreo continuo de posture gaps y alertas críticas. Se han afinado reglas de detección automatizada y se han establecido procesos claros de escalamiento, de modo que todo hallazgo relevante llegue de inmediato al equipo responsable.
2. Detección y respuesta en tiempo real

   He integrado el análisis de tráfico capturado por el WAF de Cloudflare, identificando patrones de actividad sospechosa y configurando bloqueos automáticos de IPs maliciosas. Esta fase requirió tutorías especializadas y proyectos guiados para afinar los mecanismos de mitigación y asegurar su efectividad sin afectar la operación legítima.
3. Documentación técnica y "playbooks"

   Para estandarizar la respuesta y compartir conocimiento, he desarrollado memorias técnicas detalladas de logs y creado playbooks a medida que incorporamos nuevas herramientas o procesos. Este material servirá como guía

práctica para el equipo de Cloud Security y como base para futuras capacitaciones.

4. Formación continua y desarrollo de competencias

   El plan de actividades educativas, diseñado para un ciclo de doce meses, incluyó cursos en línea de Salt, sesiones de práctica en Cloudflare y talleres de gestión de logs. Estas acciones permitieron cerrar los gaps identificados en el Inventario de Competencias, fortaleciendo tanto mis habilidades técnicas como mi capacidad de documentación y trabajo colaborativo.

1. Introducción

En el primer PAP llevé a cabo un diagnóstico exhaustivo de la administración de la postura de seguridad en la nube (CSPM) de Baxter. Durante ese periodo, analicé el flujo de detección de errores de configuración, propuse mejoras al reporte de alertas y validé integraciones con herramientas de ciberseguridad todo ello bajo la mentoría del equipo de Cloud Security. Aquella experiencia me permitió consolidar habilidades en la detección de posture gaps con Salt, en la elaboración de memorias técnicas y en la interacción con procesos reales de mitigación de riesgos.

En este segundo PAP, llevaré a cabo la implementación y operacionalización de las recomendaciones generadas previamente, así como la expansión de las capacidades de respuesta en tiempo real. El proyecto se desarrollará en el área de Cloud Security de Baxter, bajo un ciclo iterativo de doce meses que contempla ajustes en Salt, el análisis de tráfico del WAF de Cloudflare y la creación de playbooks. Mi compromiso incluirá la ejecución de las actividades planificadas, la validación continua de resultados y la documentación de cada avance para asegurar la trazabilidad y la mejora permanente.

1.1 Antecedentes

En el PAP 1, trabajé con el equipo de Cloud Security de Baxter para comprender el estado actual de las herramientas CSPM y detectar las brechas en el flujo de reporte de alertas. Ese estudio inicial reveló la necesidad de ajustar reglas de detección y de automatizar el escalamiento de hallazgos críticos. A partir de allí, diseñé una propuesta de mejora basada en mejores prácticas y en la integración con sistemas existentes.

La organización huésped sigue siendo Baxter, empresa estadounidense con sede en Deerfield, Illinois, dedicada al desarrollo de equipamiento médico. Sus principales ramas tecnológicas abarcan soluciones intravenosas, camas de hospital, sistemas de diálisis y dispositivos de monitoreo. Sus clientes son hospitales, clínicas de diálisis e instituciones de salud, tanto en mercados locales como en más de 100 países a nivel global. La misión de Baxter, "salvar y sostener vidas", inspira proyectos como este, donde la seguridad y la confiabilidad de la tecnología médica son pilares esenciales para el bienestar de los pacientes.

1.2 Justificación

Mi motivación para continuar en este PAP radica en la posibilidad de traducir el diagnóstico y las propuestas del primer proyecto en acciones concretas y resultados medibles. La oportunidad de participar en la implementación de ajustes en Salt, de

configurar bloqueos automáticos en Cloudflare y de estandarizar la respuesta mediante playbooks, se alinea directamente con mi formación en Ingeniería en Ciberseguridad y con mi objetivo de convertirme en un profesional capaz de diseñar, ejecutar y documentar soluciones de seguridad de punta a punta.

Estimo dedicar alrededor de 25 horas semanales a este proyecto incluyendo la ejecución técnica, el aprendizaje continuo y las actividades de documentación, todo ello compatible con el cumplimiento de mis materias restantes. Cuento con el apoyo de Baxter en mentorías continuas, acceso a entornos de prueba y recursos para certificaciones específicas, así como con la guía académica del Profesor PAP. La disciplina, la organización y la pasión por la ciberseguridad serán clave para cumplir los objetivos y generar un impacto real en la postura de seguridad en la nube de la organización.

1.3 Objetivos

Baxter, a través de su programa de Proyectos de Aplicación Profesional, persigue consolidar operaciones de Cloud Security innovadoras y resilientes. Con este PAP 2, la organización busca llevar a producción las optimizaciones de CSPM y nuevas capacidades de respuesta desarrolladas en el PAP 1, fortaleciendo la postura de seguridad de sus centros globales de TI en Guadalajara e India. El entregable principal será un conjunto de procesos automatizados y "playbooks" operativos que integren Salt y Cloudflare, garantizando monitoreo continuo y mitigación en tiempo real de amenazas en la nube.

Mis objetivos de aprendizaje

1. Dominio técnico profundo en operación de Salt para posture gaps, afinamiento de reglas CSPM y bloqueo automático de atacantes en Cloudflare.
2. Integración de sistemas: experimentar con flujos de datos entre CSPM, WAF y otras herramientas de seguridad para lograr una orquestación fluida.
3. Resiliencia operativa: diseñar y documentar playbooks que permitan al equipo responder con agilidad y consistencia ante incidentes reales.
4. Gestión de proyectos y colaboración: coordinar despliegues iterativos, comunicar resultados y liderar sesiones de retroalimentación en un entorno profesional real.
5. Actitud proactiva y ética: afianzar valores de responsabilidad, transparencia y compromiso con la misión de "salvar y sostener vidas" en cada decisión técnica.

Las principales competencias implicadas son:

- Técnicas: Gestión operativa de CSPM y Salt; detección y respuesta a incidentes en cloud.
- De integración: Trabajo colaborativo en equipos multidisciplinarios y comunicación con mi líder técnico.

- De actitud: Proactividad, disciplina en el seguimiento de procesos y compromiso ético en la toma de decisiones.

1.4 Contexto

Este PAP 2 se enmarca como un proyecto de mejora de procesos dentro del área de Cloud Security de Baxter. Está dirigido principalmente al equipo interno de TI y seguridad, aunque repercutirá en la fiabilidad de los servicios médicos para hospitales e instituciones de salud en más de 100 países (beneficio global). A través de la automatización y estandarización de reportes y bloqueos, se espera reducir tiempos de respuesta y disminuir el riesgo operativo en entornos cloud.

Mi rol es el de Intern en Cloud Security, y mis funciones incluyen:

- Ejecutar ajustes en Salt para monitorizar posture gaps.
- Configurar y probar reglas en el WAF de Cloudflare para mitigar ataques.
- Diseñar e implementar playbooks de respuesta a incidentes.
- Documentar procedimientos y capacitar al equipo en las nuevas herramientas.

1.5 Inventario de Competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	**Gestión Operativa de CSPM y Salt**	4	3	1	4	A
1.1	Monitoreo de posture gaps y alertas con Salt	4	3	1	4	A
1.2	Configuración y tuning de reglas de detección automatizada	4	2	2	4	A
1.3	Priorización y escalamiento de hallazgos críticos	3	3	0	4	A
2	**Detección y Respuesta a Incidentes en Cloud**	4	3	1	4	A
2.1	Análisis de tráfico y actividades sospechosas en entornos cloud	4	3	1	4	A
2.2	Implementación de bloqueos de atacantes y mitigación inmediata	4	2	2	4	A
3	**Documentación y Memorias Técnicas**	3	1	2	3	M
3.1	Generación y gestión de logs técnicos detallados para documentar	3	1	2	3	M
3.2	Elaboración de reportes técnicos "playbooks"	3	2	1	3	M

1.6 Plan Educativo

No.	Actividad Educativa	Tipo Actividad	Prereq	Total Hrs	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	9	10	11	12
1.1	Revision de cursos gratuitos y documentación de la herramienta SALT	Cursos en linea		30	abr-25	may-25												
1.2	Sesiones prácticas de escalamiento de alertas críticas	Tutoría		15	may-25	jul-25												
2.1	Casos de Análisis de tráfico sospechoso capturado por el WAF de Cloudflare	Proyecto guiado		25	ago-25	oct-25												
2.2	Tutoria en Cloudflare sobre bloqueo de atacantes y mitigación inmediata	Proyecto guiado	2.1	20	ago-25	mar-26												
2.3	Tuneos espontaneamente necesarios de reglas de detección de trafico sospechoso en Cloudflare	Tutoría		30	ago-25	mar-26												
3.1	Gestión y selección de logs técnicos	Tutoría		15	ene-26	mar-26												
3.2	Creación de “Playbooks” a medida que creamos herramientas o procesos	Proyecto guiado	3.1	30	ene-26	mar-26												

1.7 Entregables

Durante este segundo PAP se esperan los siguientes entregables, producidos de manera individual y colaborativa:

1. Ajustes operativos en Salt para CSPM
   Conjunto de scripts y configuraciones actualizadas que garantizan el monitoreo continuo de posture gaps y la generación automática de alertas.
2. Reglas de bloqueo en Cloudflare WAF
   Definición y despliegue de reglas afinadas para mitigar tráfico malicioso en tiempo real, junto con un informe de pruebas de efectividad.
3. Playbooks de respuesta a incidentes
   Documentos “vivos” que describen paso a paso los procedimientos para identificar, contener y remediar distintos tipos de alertas y ataques en la nube.
4. Informe de resultados y métricas de mejora
   Resumen ejecutivo con indicadores clave (por ejemplo, estadísticas de detección y bloqueo) que demuestra el impacto de las implementaciones.

1.8 Involucrados

- Área de Cloud Security (Equipo Interno)
  Responsable de recibir, validar y operar los entregables, colaboran estrechamente en pruebas y ajustes.
- Mentor Técnico / Gerente PAP (Alex)
  Supervisa el avance, valida los criterios de calidad y aprueba los entregables formales.

- Equipo de Infraestructura y Operaciones Cloud
  Integra los cambios en los entornos de producción y gestiona el aprovisionamiento de recursos necesarios.
- Profesor / Coordinación PAP-DESI
  Recibe informes periódicos, evalúa el cumplimiento de objetivos académicos y garantiza la alineación con los requerimientos del ITESO.

Cada uno de estos actores contribuye a la definición, revisión y uso de los entregables, y se verá directamente beneficiado por la mejora en los tiempos de detección, la robustez de la respuesta y la calidad de la documentación.

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

Inicio

Se definen los objetivos de este PAP 2: implementar las mejoras de CSPM y las capacidades de respuesta en tiempo real diseñadas en el PAP 1. Se revisan los entregables principales scripts de Salt, reglas de Cloudflare, playbooks y memorias técnicas y se obtiene la aprobación de mi mentor técnico para arrancar el ciclo de doce meses.

Planificación

Se elabora un cronograma mensual que incluye las actividades del Plan de Desarrollo Profesional (cursos en línea, tutorías y proyectos guiados) y las fases de despliegue en entornos de prueba y producción. Cada tarea se asigna con fechas de inicio y término, recursos involucrados y prerequisitos, garantizando alineación con los compromisos académicos y operativos.

Ejecución

Ajustes en Salt: desarrollo y despliegue de scripts para monitorear posture gaps.
Configuración de WAF: afinamiento de reglas en Cloudflare y pruebas de bloqueo automático.
Creación de playbooks: documentación paso a paso de respuestas a incidentes.
A lo largo de la ejecución, se levantan tickets internos para cada cambio, se registran resultados de pruebas y se actualiza la documentación en repositorios compartidos.

Seguimiento y Control

Reuniones semanales con el mentor técnico vía Teams para revisar avances, bloqueos y acciones correctivas.
Actualización continua de indicadores (por ejemplo, tiempo medio de bloqueo, número de posture gaps reducidos) en un dashboard interno.
Correo y carpeta compartida: registro de decisiones, feedback y ajustes al plan.

Cierre

Al término del periodo, se consolidan todos los scripts, reglas, playbooks y memorias técnicas en un paquete entregable. Se presenta un informe final con métricas de mejora y recomendaciones, y se realiza una sesión de transferencia de conocimiento al equipo de Cloud Security.

2.2 Sustento Teórico y Metodológico

Baxter no emplea un proceso formal de metodologías rígidas para producir sus entregables de seguridad en la nube, en cambio, sigue procedimientos internos flexibles basados en:

1. Ciclo iterativo de validación
   Cada cambio propuesto se prueba en entornos controlados, se recaba feedback y se ajusta antes de pasar a la siguiente iteración, permitiendo una mejora continua sin interrumpir la operación.
2. Gestión de cambios y control documental
   Se utiliza un sistema de tickets (interno) para registrar solicitudes de ajuste, aprobaciones de configuración y resultados de pruebas. Los documentos y scripts se versionan en repositorios compartidos.
3. Comunicación estructurada
   Aunque no se sigue Scrum formalmente, la coordinación ocurre mediante reuniones semanales, updates por correo y registro de actas en Teams, lo que garantiza transparencia y trazabilidad de cada decisión.

Esta combinación de prácticas iteraciones breves, gestión de cambios y comunicación documentada asegura que los entregables cumplan con los estándares de calidad y seguridad de Baxter sin depender de marcos externos rígidos.

2.3 Descripción del Proyecto

El PAP 2 consiste en llevar a producción un conjunto de sub-entregables que, secuencialmente, construyen la solución final:

1. Scripts de Salt para CSPM
   - Desarrollo, prueba y despliegue de configuraciones automatizadas para monitorear posture gaps.
   - Entrega de un paquete de scripts versionados.
2. Reglas afinadas en Cloudflare WAF
   - Definición, prueba y despliegue en producción de reglas de bloqueo de IP maliciosas.
   - Informe de efectividad con métricas de tráfico benigno vs. malicioso.
3. Playbooks
   - Documentos vivientes que describen flujos de contención y remediación ante distintos tipos de alertas.
   - Sesiones de validación con el equipo de operaciones.
4. Memorias técnicas y dashboard de métricas

- Repositorio organizado de logs y un panel interno que muestra indicadores de desempeño.

Estos sub-entregables se integran progresivamente: primero en entornos de pre-producción y, finalmente, en producción. El proyecto funciona como un módulo independiente dentro de la iniciativa global de hardening de Cloud Security, pero se alinea con otras fases de mejora continua de la organización.

Recursos clave

- Salt y algunos scripts
- Cloudflare
- Teams y carpetas compartidas (para versionado y documentación)

2.4 Tipo de Proyecto

El ciclo de vida de este PAP 2 sigue un enfoque iterativo. Este modelo permite validar rápidamente cada cambio, por ejemplo, un nuevo script de Salt o una regla de Cloudflare, recolectar retroalimentación y corregir desviaciones antes de avanzar a la siguiente iteración.

Otras características específicas del proyecto incluyen:

- Configuración y scripting: desarrollo de scripts de Salt para posture gaps y automatización de alertas.
- Pruebas de seguridad: diseño y ejecución de casos de prueba para validar reglas de bloqueo en el WAF de Cloudflare.
- Documentación técnica: elaboración de playbooks y memorias técnicas, así como gestión de logs para soporte forense.
- Integración de sistemas: orquestación de flujos de datos entre CSPM, WAF y repositorios de incidentes.

Este enfoque evolutivo hace que cada componente se refine de forma progresiva, alineando la entrega continua de valor con la mejora permanente de la postura de seguridad en la nube de Baxter.

2.5 Plan de Trabajo

A partir de mi Inventario de Competencias, estas son las habilidades clave que debo desarrollar para producir los entregables del PAP 2

No.	Competencia	Nivel Adquirido al Inicio	Nivel Objetivo al final PAP	Objetivo final PAP	Prior
1	Gestión operativa de CSPM y Salt	3	4	1	A
1.1	Monitoreo de posture gaps y alertas con Salt	3	4	1	A
1.2	Configuración y tuning de reglas de detección automatizada	2	4	2	A
1.3	Priorización y escalamiento de hallazgos críticos	3	4	1	A
2	Detección y respuesta a incidentes en Cloud	3	4	1	A
2.1	Análisis de tráfico y actividades sospechosas en entornos cloud	3	4	1	A
2.2	Implementación de bloqueos de atacantes y mitigación inmediata	2	4	2	A
3	Documentación y memorias técnicas	1	3	2	M
3.1	Generación y gestión de logs técnicos detallados	1	3	2	M
3.2	Elaboración de reportes técnicos y playbooks	2	3	1	M

No.	Actividad Educativa	Encargado	Total Hrs	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	9	10	11	12	Obj
1	Gestión Operativa de CSPM y Salt	Emiliano (Intern)	—	—	—													
1.1	Revisión de cursos gratuitos y documentación de la herramienta Salt	Emiliano (Intern)	30	abr-25	may-25													
1.2	Sesiones prácticas de escalamiento de alertas críticas	Emiliano & Alex (Mentor)	15	may-25	jul-25													
2	Detección y Respuesta a Incidentes en Cloud	Emiliano (Intern)	—	—	—													
2.1	Casos de análisis de tráfico sospechoso capturado por el WAF de Cloudflare	Emiliano (Intern)	25	ago-25	oct-25													
2.2	Tutoría en Cloudflare sobre bloqueo de atacantes y mitigación inmediata	Emiliano & Kumar	20	ago-25	mar-26													
2.3	Tuneos espontáneos de reglas de detección de tráfico sospechoso en Cloudflare	Emiliano (Intern)	30	ago-25	mar-26													
3	Documentación y Memorias Técnicas	Emiliano (Intern)	—	—	—													
3.1	Gestión y selección de logs técnicos	Emiliano (Intern)	15	ene-26	mar-26													
3.2	Creación de playbooks a medida que implementamos nuevas herramientas o procesos	Emiliano (Intern)	30	ene-26	mar-26													

2.6 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 ciberamenazas,	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 ciberamenazas,	Emiliano (yo)

2.7 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)
Becario Cloud Security (Emiliano)	Avances del proyecto y consultas específicas sobre tareas	Profesor PAP	Canvas, junta virtual	Mensual (m)

2.8 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	Scripts de Salt para posture gaps	Mentor Técnico (Alex)	Código limpio y comentado para la automatización de envío de alertas generadas por salt.	Pruebas de envío
Becarios Cloud Security	Reglas afinadas en Cloudflare WAF	Mentor Técnico (Alex)	Bloqueos efectivos en sandbox sin falsos positivos; documentación de cambios; aprobación de métricas de desempeño.	Despliegue en producción y monitorización continua
Becarios Cloud Security	Playbooks de respuesta a incidentes	Mentor Técnico (Alex)	Procedimientos claros, paso a paso, validación práctica, feedback positivo.	Carpeta compartida de Cloud Security e interesados.
Becarios Cloud Security	Memorias técnicas y dashboard de métricas	Mentor Técnico (Alex)	Panel con indicadores consistencia con objetivos de mejora (reducción de gaps).	Presentación de resultados y cierre de fase

2.9 Seguimiento y Control

Monitoreo interno con el equipo de Cloud Security

- Reuniones semanales (vía Teams):
  - Revisión de avances en scripts, reglas y playbooks.
  - Evaluación de métricas (estadísticas de bloqueo, posture gaps reducidos).
  - Identificación de bloqueos técnicos y reasignación ágil de tareas.
  - Registro de acciones correctivas en la carpeta de control de cambios.
- Dashboard de métricas (continuo):

    - Visualización en tiempo real de indicadores clave.
    - Actualización automática tras cada despliegue.
- Comunicación puntual (correo/Teams):
    - Notificación inmediata de incidentes críticos.
    - Aprobaciones rápidas para cambios urgentes.

Interacciones con Coordinación PAP y Profesor PAP

- Revisiones del reporte PAP con el Profesor PAP:
    - Presentación de estado de entregables y métricas.
    - Ajustes según retroalimentación.

2.10 Cierre del Proyecto

Al concluir la fase de implementación de PrismaCloud y el reporte de alertas, se llevó a cabo un proceso de cierre parcial que incluyó:

1. Entrega-recepción
    - Se presentaron los scripts, reglas y playbooks al Mentor Técnico y al Equipo de automatizaciones.
    - Se verificó que todos los entregables cumplían con alcance, calidad y claridad para darle paso a una automatización masiva para el envío de las alertas salidas de PrismaCloud y nosotros concentrarnos en otras herramientas.
2. Evaluación Final
    - Sesión de retroalimentación con Alex (Mentor Técnico), donde se evaluó nuestro desempeño en términos de iniciativa, calidad técnica y colaboración.

Con estos cierres parciales, se formalizó la transición a la siguiente fase del PAP 2, garantizando la continuidad y la correcta integración de los resultados en el entorno productivo de Baxter.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

En esta segunda etapa de mi participación en el PAP, consolidé y amplié los entregables iniciales para que pasaran de ser análisis exploratorios a soluciones funcionales que están siendo evaluadas e implementadas dentro del entorno de producción. Los principales productos obtenidos son:

1. Refinamiento del flujo de priorización de alertas críticas en CSPM y Salt
   Se diseñó y documentó una propuesta optimizada para la priorización y escalamiento de hallazgos de seguridad. Esta mejora permite que los errores críticos en la configuración cloud sean identificados y asignados de forma más eficiente, disminuyendo los tiempos de respuesta y reduciendo el ruido operativo (el cual ha sido una queja entre los system owners).
2. Tuneo e implementación progresiva de reglas de detección automatizada
   Se realizaron ajustes personalizados a reglas de detección en herramientas como Cloudflare y Salt, con base en el comportamiento observado, necesidades de la aplicación correspondiente y en base a tendencias actuales de amenazas. Estos tuneos han mejorado la precisión de las alertas, disminuyendo los falsos positivos y permitiendo una gestión más eficiente del riesgo.
3. Casos de análisis de tráfico sospechoso y mitigación proactiva
   Manejo de casos reales de tráfico malicioso detectado por el WAF de Cloudflare, incluyendo análisis de patrones, propuestas de mitigación y pruebas de bloqueo. Este producto ha servido como insumo para la toma de decisiones del equipo de respuesta a incidentes.
4. Primeros "playbooks" de operación para Cloud Security en Baxter
   Se inició la elaboración de documentos tipo playbook que sistematizan acciones concretas frente a incidentes o hallazgos específicos. Esta documentación servirá como referencia rápida para nuevos integrantes del equipo y facilitará la estandarización de respuestas frente a escenarios comunes.

3.2 Estimación del Impacto

Los entregables desarrollados durante este segundo PAP tienen un impacto directo en la capacidad del equipo de Cloud Security para responder con mayor precisión, velocidad y consistencia ante los desafíos de seguridad en los entornos cloud de Baxter. La mejora en el filtrado de alertas críticas y la reducción de falsos positivos no solo ha optimizado los recursos del equipo, sino que también contribuye a minimizar el riesgo de exposición de activos críticos de la empresa.

La elaboración de playbooks representan un paso hacia la madurez operativa del área, permitiendo que el conocimiento no dependa exclusivamente de la experiencia de cada individuo, sino que se institucionalice como parte de la cultura técnica del equipo. Además, la incorporación de logs y análisis técnicos en un repositorio interno permanente ofrece un punto de partida para futuros ejercicios de respuesta, auditoría o mejora.

Prospectivamente, el impacto de estos entregables tiene dos principales objetivos, el mejoramiento operativo, al optimizar procesos internos de seguridad, y mejoramiento estratégico, al fortalecer la resiliencia y capacidad de adaptación del equipo ante amenazas emergentes. Este PAP no solo me permitió aplicar mis conocimientos, sino que aportó valor real a una infraestructura global de tecnología crítica.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

1. Gestión avanzada de CSPM y Salt
   Pasé de identificar posture gaps a lograr su automatización. Ahora configuro scripts que priorizan y escalan alertas con muy poca intervención manual, una capacidad que antes consideraba distante.
2. Detección y respuesta en entornos cloud
   Aprendí a interpretar patrones de tráfico malicioso en Cloudflare y a desplegar bloqueos automáticos seguros. Esta destreza transformó mi visión de la defensa: ya no es reactiva, sino proactiva y basada en evidencia.
3. Documentación operativa y playbooks
   Crear "playbooks" me enseñó a traducir conocimientos técnicos en guías prácticas. Descubrí que la claridad en la documentación acelera la incorporación de posibles nuevos integrantes y mejora la consistencia de la respuesta.
4. Visión estratégica y toma de decisiones
   Comprendí que cada ajuste técnico debe conectar con metas de negocio reducir riesgo operativo, mejorar tiempos de mitigación. Ahora puedo diseñar, planificar y defender propuestas con un enfoque que integra lo técnico y lo estratégico desde un punto de vista más cercano a lo que está pasando en la seguridad de la nube en Baxter.

4.2 Aprendizajes Sociales

Todo este PAP me ha dejado claro que una mejora técnica va mucho más allá de lo que pensaba, esto también impacta directamente en la vida de quienes dependen de sistemas sanitarios. Al reforzar la seguridad de Baxter, contribuimos a:

1. Protección de datos sensibles
   Asegurar la confidencialidad de historiales médicos y datos de pacientes reduce el riesgo de filtraciones que pudieran afectar su privacidad y bienestar.
2. Mayor confiabilidad operativa
   Al disminuir interrupciones por alertas falsas y mejorar la rapidez de respuesta a incidentes reales, hospitales y clínicas pueden mantener sus servicios en línea sin paros inesperados.
3. Calidad de atención al paciente
   Sistemas más estables y seguros permiten que médicos y enfermeras

confíen en sus herramientas digitales, enfocándose en el cuidado y no en problemas técnicos.

4.3 Aprendizajes Éticos

1. Alineación de valores
   Mis principios se alinean con la misión de Baxter "salvar y sostener vidas". Aunque no lidié con datos personales de pacientes, sí trabajé con infraestructura que sostiene servicios médicos: un descuido podía traducirse en interrupciones o brechas en sistemas vitales.
2. Dilemas de comunicación
   Mi formación y valores me impulsaron a no solo limitarme a ejecutar scripts, sino a garantizar que cada alerta llegara a las personas correctas. Hubo ocasiones en que, al ver que una alerta de alto riesgo, esta no tenía información de contacto que nos llevara hacía los responsables de la aplicación, entonces, decidíamos elevarla personalmente al equipo de operaciones, a pesar de que esto implicaba cuestionar flujos establecidos.
3. Responsabilidad colectiva
   Ese acto de insistencia fue un ejercicio de transparencia y responsabilidad colectiva. Aprendí que la ética profesional en ciberseguridad no solo consiste en detectar fallas técnicas, sino en esforzarnos, para que la información llegue efectivamente a quienes pueden remediarlas.

4.4 Aprendizajes Personales

1. Autoconocimiento y confianza
   Descubrí que puedo adaptarme a escenarios de alta presión, diseñar reglas, documentar playbooks y compartirlos ante compañeros me dio seguridad en mis ideas y en mi capacidad de liderazgo técnico, además, ser reconocido por mi trabajo en algunas reuniones me hizo sentir capaz de continuar con este tipo de tareas y responsabilidades.
2. Relaciones enriquecidas
   Valorar la diversidad de pensamiento en el equipo me enseñó a preguntar más y asumir que las mejores soluciones surgen del diálogo.
3. Madurez y resiliencia
   Afrontar atrasos o rechazos iniciales (por falsos positivos, por ejemplo) me enseñó a ver el fracaso como fuente de mejora continua y a mantener la calma bajo presión.

4.5 Tareas Aprendidas

Estos fueron algunos factores que impulsaron el éxito

1. Comunicación constante: Canales abiertos con mi mentor y colegas.
2. Flexibilidad: Ajustar reglas y scripts en tiempo real según resultados de pruebas.
3. Responsabilidad compartida: La disposición del equipo a colaborar combinó aportes técnicos para lograr algunos objetivos.

Sin embargo, identifiqué áreas de mejora como:

1. Coordinación en momentos críticos: Acelerar aprobaciones urgentes mediante solicitar micro-reuniones.
2. Retroalimentación más ágil: Solicitar reviews parciales para evitar retrabajos y modificaciones extensas.
3. Documentación incremental: Registrar cada cambio al instante para no acumular documentación pendiente al cierre.

4.6 Desarrollo Profesional

Al diseñar mi Proyecto Individual de Desarrollo Profesional, consolidé una visión clara de mi futuro, convertirme en un Arquitecto de Cloud Security que combine automatización avanzada y modelos de IA para fortalecer defensas en entornos críticos.
Esta hoja de ruta me ha permitido descubrir nuevas alternativas y priorizar mis esfuerzos hacia roles de alto impacto.

Elementos básicos de mi nicho de desarrollo

1. Tareas tecnológicas favoritas
    - Automatización de seguridad cloud: diseñar pipelines que integren herramientas de CSPM, WAF y orquestación de contenedores (Docker/Kubernetes).
    - Modelos de Inteligencia Artificial para detección de anomalías: implementar prototipos ML que analicen logs y comportamientos inusuales en tiempo real.
    - Scripting y desarrollo de herramientas internas: crear scripts en Python que aceleren respuestas ante incidentes.
2. Áreas tecnológicas de mayor destreza
    - Posture Management en la nube (AWS, Azure).
    - Scripting y automatización (Python).
    - Documentación técnica.

3. Mercado con mayor crecimiento
    - Cloud Security "as a Service" para pymes de salud y servicios críticos.
    - Soluciones de ML/IA en ciberseguridad, especialmente detección predictiva.
    - DevSecOps y orquestación de contenedores para entornos heterogéneos.

Pasos y estrategia hacia la posición objetivo y esfuerzo requerido

No.	Actividad Educativa	Tipo Actividad	Prereq	Total Hrs	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	9	10	11	12
1.1	Revision de cursos gratuitos y documentación de la herramienta SALT	Cursos en linea		30	abr-25	may-25												
1.2	Sesiones prácticas de escalamiento de alertas críticas	Tutoría		15	may-25	jul-25												
2.1	Casos de Análisis de tráfico sospechoso capturado por el WAF de Cloudflare	Proyecto guiado		25	ago-25	oct-25												
2.2	Tutoria en Cloudflare sobre bloqueo de atacantes y mitigación inmediata	Proyecto guiado	2.1	20	ago-25	mar-26												
2.3	Tuneos espontaneamente necesarios de reglas de detección de trafico sospechoso en Cloudflare	Tutoría		30	ago-25	mar-26												
3.1	Gestión y selección de logs técnicos	Tutoría		15	ene-26	mar-26												
3.2	Creación de "Playbooks" a medida que creamos herramientas o procesos	Proyecto guiado	3.1	30	ene-26	mar-26												

Tendencias del mercado y cambios esperados

- Expansión del Cloud Security Posture Management: cada vez más empresas, incluso en sectores regulados, adoptan CSPM como estándar.
- Crecimiento de la IA defensiva: la detección predictiva se convertirá en requisito para responder a amenazas sofisticadas.
- Énfasis en DevSecOps: la seguridad se integrará desde el diseño de pipelines CI/CD.

Proyectos y posiciones visualizadas

- Arquitecto de Cloud Security en Baxter o en un proveedor de servicios gestionados para salud.
- Consultor de IA para Ciberseguridad en empresas como Palo Alto Networks o startups especializadas en ML defensivo.
- Desarrollo de un laboratorio de ML+WAF que ofrezca detección de anomalías.

Factores clave para invertir mi esfuerzo

1. Alineación ética: contribuir a "salvar y sostener vidas" mediante defensas robustas en la nube.
2. Demanda de mercado: creciente necesidad de expertos en CSPM y automatización IA.
3. Satisfacción profesional: combinar creatividad técnica y análisis profundo en proyectos de alto valor.

Este plan me guiará durante los próximos cinco años, asegurando que mis acciones como, certificaciones, proyectos y networking, estén alineadas con mi meta de liderar la arquitectura de seguridad en la nube.

5. Conclusiones

Haber documentado detalladamente mis dos ciclos de PAP fue un ejercicio invaluable, al plasmar experiencias, aprendizajes y reflexiones en un solo reporte, consolido mi conocimiento y me preparo para exponer de manera clara y contundente mis aportes, tanto ante la comunidad académica como frente a mis colegas en Baxter.

Más allá de los scripts y la seguridad, lo que más valoro son las lecciones de resiliencia y autoconocimiento que surgieron al enfrentar desafíos reales. Aprendí que adaptarme bajo presión me fortaleció no solo como técnico, sino también como persona, descubrí que tengo la capacidad de mantener la calma y seguir adelante incluso cuando todo parecía urgente.

La experiencia reforzó también mi confianza, pasé de dudar de mis ideas frente a líderes a defender con convicción mis propuestas de mejora. Esa transición de "estudiante inseguro" a "profesional que aporta" me hizo entender que el valor de mi voz se encuentra tanto en el conocimiento que tengo como en la forma de comunicarlo.

En cuestión de las sesiones del PAP, cada reunión, y, en particular, aquellas pocas sesiones de reflexión personal o tips personales que tuvimos, amplió mi perspectiva, mostrándome cómo vincular mis aprendizajes con mi propio proyecto de vida. Reflexiono con gratitud sobre esas sesiones de aprendizaje personal, fueron espacios para compartir nuestros planes de vida y recibir tips o feedback honesto.

Me ayudaron a ver áreas ocultas de mejora en mi comunicación, mi gestión del tiempo y mi manera de afrontar el error. Creo firmemente que incorporar más de estas sesiones enriquecería el PAP para futuros estudiantes.

Al cerrar esta etapa, siento una profunda satisfacción, el esfuerzo invertido se vio reflejado en mi crecimiento emocional, en mi capacidad de trabajo en equipo y en mi visión de futuro.