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

IT LEGAL SERVICES

PRESENTA

Alumno: ICI, Andrés Alejandro Váquez Chávez

Profesor PAP: Juan Manuel Islas Espinoza

Tlaquepaque, Jalisco, Agosto 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

El presente trabajo tiene como objetivo desarrollar competencias prácticas en la aplicación de la norma ISO 27001, enfocada en la gestión de la seguridad de la información dentro del entorno empresarial con base a la ley mexicana.
El alcance se centró en la comprensión y aplicación de los principales requisitos de la norma, desde la planeación de un proyecto de seguridad hasta la implementación y verificación de controles. Este trabajo no se limita a la teoría, sino que busca vincular la normativa con actividades prácticas en el ámbito del PAP, especialmente en la identificación de riesgos, la elaboración de planes de acción y la validación de medidas de seguridad.
La metodología consiste en tres etapas.

1. Análisis inicial: revisión de la situación actual, identificación de brechas y requerimientos de la organización respecto a ISO 27001.
2. Planificación y ejecución: diseño de un plan de acción con actividades educativas, autoestudio, tutorías y prácticas en la empresa para implementar controles de seguridad.
3. Seguimiento y verificación: corroboración de la implementación mediante revisión de evidencias y retroalimentación del responsable del proyecto.

De esta forma, el trabajo permitió integrar conocimientos técnicos y normativos, desarrollando habilidades en gestión de seguridad y cumplimiento regulatorio. Al finalizar, se logró consolidar un aprendizaje aplicado que fortalece la preparación profesional en el campo de la ciberseguridad.

1. Introducción

Durante el periodo del PAP, se desarrollará un proyecto orientado a la aplicación de la norma ISO 27001 dentro de la organización IT Legal Services. El trabajo se enfocará en la planeación, implementación y verificación de controles de seguridad de la información que permitan alinear las prácticas internas con los requisitos de la norma.

El proyecto tendrá como punto de partida un diagnóstico de la situación actual en materia de seguridad de la información, a partir del cual se identificarán brechas y áreas de oportunidad. Posteriormente, se diseñará un plan de acción con actividades que incluirán la construcción de políticas, la implementación de controles técnicos y administrativos, y la revisión de la efectividad de las medidas adoptadas.

De manera complementaria, se realizará un proceso de documentación y validación de cada fase, con el propósito de garantizar la trazabilidad de las acciones y su alineación con el marco normativo aplicable.

Este proyecto contribuirá al fortalecimiento de las competencias profesionales del alumno en materia de gestión de seguridad de la información y apoyará a la empresa en el cumplimiento de buenas prácticas internacionales en ciberseguridad.

Antecedentes

La organización huésped es IT Legal Services, una empresa enfocada en proveer soluciones integrales de ciberseguridad y gestión de la información.

Sus principales ramas tecnológicas se concentran en la seguridad informática, la gestión de incidentes de ciberseguridad, la investigación forense digital y la respuesta ante ataques de ransomware. Estas áreas se complementan con la asesoría en cumplimiento normativo y la implementación de marcos de seguridad como la norma ISO 27001.

La empresa ofrece servicios especializados que incluyen análisis forense digital, mitigación y recuperación tras incidentes de ransomware, consultoría en normativas de protección de datos, auditorías de seguridad, y capacitación en mejores prácticas de ciberseguridad. Estos servicios están diseñados tanto para prevenir riesgos como para responder eficazmente a incidentes de alto impacto.

La misión de IT Legal Services se inspira en proteger la integridad de la información, salvaguardar los activos digitales de las organizaciones y promover un entorno confiable en el uso de la tecnología, basándose en valores de ética, responsabilidad y compromiso social.

Sus clientes incluyen organizaciones de los sectores de servicios, finanzas, manufactura, gobierno y PYMES, que requieren apoyo en la protección de su infraestructura digital. Los principales mercados de la empresa se encuentran en el ámbito nacional, con proyección hacia servicios regionales en América Latina, adaptándose a la creciente demanda de soluciones de seguridad y cumplimiento normativo.

Justificación

Durante mi participación en este proyecto PAP, buscaré fortalecer mis competencias en ciberseguridad, específicamente en los aspectos relacionados con ISO 27001 y regulaciones en materia de protección de datos. Reconozco que estas áreas representan un reto para mí, ya que mi experiencia previa se ha enfocado más en el ámbito técnico de la seguridad, mientras que los marcos normativos, estándares internacionales y procesos de cumplimiento requieren un conocimiento más estructurado.

El proyecto me permitirá profundizar en la comprensión de la norma ISO 27001, así como en la aplicación práctica de políticas, controles y procedimientos que apoyan la gestión de la seguridad de la información en una organización. Además, espero mejorar mis habilidades en la interpretación y aplicación de regulaciones vigentes, lo que contribuirá a desarrollar una visión más integral de la ciberseguridad, combinando tanto el enfoque técnico como el normativo.

1.1 Objetivos

Explica El propósito de IT Legal Services al realizar proyectos PAP es fortalecer el vínculo entre la academia y el ámbito profesional, ofreciendo a los estudiantes un espacio donde puedan aplicar sus conocimientos en un entorno real. Con estos proyectos, la empresa busca apoyar su misión de impulsar la seguridad de la información, al mismo tiempo que contribuye a la formación de futuros profesionales capaces de enfrentar los retos de la ciberseguridad. Asimismo, estos proyectos permiten a la organización detectar talento, aportar a la comunidad académica y enriquecer sus propias prácticas con la colaboración de nuevas perspectivas.

Por mi parte, mi principal objetivo durante este PAP es desarrollar y reforzar mis habilidades en ciberseguridad, especialmente en los temas relacionados con ISO

27001, cumplimiento normativo y regulaciones de protección de datos, que identifico como áreas de mejora en mi formación. Además, espero ganar experiencia práctica en la gestión de incidentes de seguridad y la investigación forense digital, con el fin de integrar el conocimiento técnico con el marco regulatorio. Este periodo representa una oportunidad para construir una visión más completa de la seguridad de la información, que me ayude a crecer profesionalmente y a aportar valor en mi futuro desempeño laboral.

Contexto

El PAP en el que participaré corresponde al Área de Seguridad de la Información de IT Legal Services, con enfoque específico en la implementación y cumplimiento de la norma ISO 27001, así como en actividades de análisis forense digital relacionadas con la investigación de incidentes de seguridad y respuesta a ataques como el ransomware.

El tipo de proyecto en el que estaré involucrado corresponde a la Mejora de Procesos y Apoyo a Áreas Operativas, ya que busca fortalecer las prácticas internas de seguridad de la información mediante la alineación con estándares internacionales y la incorporación de metodologías de investigación forense para casos reales de incidentes.

Mi rol dentro del proyecto será el de intern (becario). Como estudiante participante en el PAP, mis funciones consistirán en apoyar la planeación y documentación de controles de ISO 27001, colaborar en la elaboración de planes de acción de seguridad, asistir en la recolección y análisis de evidencias digitales durante procesos de investigación forense, y contribuir a la validación de medidas de seguridad implementadas. Este rol me permitirá combinar conocimientos técnicos y normativos para aportar valor a la organización y, al mismo tiempo, fortalecer mis competencias profesionales en ciberseguridad.

Inventario de Competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	**Seguridad en redes**					
1.1	Configuracion Firewalls	4	4	0	4	2
1.2	Monitoreo de trafico	4	4	0	4	2
1.3	Segmentacion de redes	4	3	1	4	2
2	**Normativas de ciberseguridad**					
2.1	Conocimiento de la Ley Federal de Proteccion de Datos	5	2	3	5	5
2.2	Conocimiento ISO 27001	5	2	3	5	5
3	**Programacion para ciberseguridad**					
3.1	Utilizacion de librarias para scripts	4	3	1	4	2
3.2	automatizaciones de busquedas en internet	4	3	1	4	2
4	**Ethical hacking**					
5	reconocimiento	2	4	2	5	2
6	enumeracion	2	4	2	5	2
7	analisis de vulnerabilidades	2	4	1	4	2
8	explotacion	2	3	1	4	2

1.6 Plan Educativo

No.	Actividad Educativa	Tipo Actividad	Total Hrs	Fecha Inicio	Fecha Término	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Obj
No.	**Actividad Educativa**	**Tipo Actividad**	**Total Hrs**	**Fecha Inicio**	**Fecha Término**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**Obj**
12	**Conocimiento de la Ley Federal de Protección de Datos**	Curso en línea + Autoestudio	20	Semana 1	Semana 4	X	X	X	X													2
12.1	Planeación de proyecto	Tutoría + Taller	10	Semana 2	Semana 5		X	X	X	X												2
12.2	Análisis de situación actual	Práctica en empresa	15	Semana 5	Semana 7					X	X	X										3
13	**Conocimiento ISO 27001**	Curso en línea + Práctica	25	Semana 6	Semana 12						X	X	X	X	X	X						3
13.1	Construcción de plan de acción	Taller + Autoestudio	10	Semana 7	Semana 9							X	X	X								3
13.2	Implementar plan de acción	Práctica en empresa	20	Semana 9	Semana 13									X	X	X	X	X				4
13.3	Corroborar implementación	Práctica en empresa	15	Semana 13	Semana 16													X	X	X	X	4

1.7 Entregables

Los entregables programados para este periodo de PAP aún no se encuentran totalmente definidos, ya que varían en función de las necesidades específicas de cada cliente y de la naturaleza de los proyectos en los que se brinde apoyo. En el área de ISO 27001 y de investigación forense, los entregables pueden incluir desde documentación de planes de acción y reportes técnicos, hasta la participación en análisis de incidentes de seguridad y propuestas de mejora en procesos de cumplimiento normativo.

Es importante señalar que debido a que la empresa mantiene un alto nivel de confidencialidad en los servicios que presta, el detalle de los subentregables y productos finales no puede especificarse de manera abierta en este documento. En todo caso, estos se ajustarán a lo establecido con mi líder técnico y estarán orientados a apoyar las actividades de seguridad de la información y respuesta a incidentes conforme a los lineamientos internos de la organización.

1.8 Involucrados

Líder del proyecto:

- Juan Carlos Durón

Equipo de trabajo:

- Juan Carlos Durón
- Mateo de la Torre
- Andrés Vázquez

Cliente externo:

- La información no se comparte por motivos de confidencialidad, debido a la delicadeza de ciertas situaciones con clientes.

Áreas de apoyo dentro del PAP:

- Forense digital (área solicitada de manera principal)
- ISO 27001 y cumplimiento normativo

1. Desarrollo del Proyecto PAP

El desarrollo del proyecto PAP en IT Legal Services se administrará mediante un esquema de supervisión directa por parte del líder de proyecto, en este caso el Mtro. Juan Carlos Durón, quien será el responsable de validar los avances y orientar las actividades en función de las prioridades de la organización y de los clientes atendidos. La coordinación del equipo, conformado por el líder técnico, el alumno y los colaboradores designados, permitirá asegurar que las tareas se ejecuten conforme a los tiempos y necesidades establecidos, siempre bajo los lineamientos de confidencialidad que exige la empresa.

El seguimiento del Proyecto de Desarrollo Educativo se llevará a cabo en paralelo, considerando las competencias definidas en el Inventario de Competencias. Se dará especial énfasis a las actividades relacionadas con la implementación de ISO 27001 y al apoyo en procesos de análisis forense digital, áreas que forman parte del plan de formación personal del alumno. Los avances serán revisados periódicamente con el líder técnico, quien proporcionará retroalimentación y ajustes necesarios para garantizar que las metas de aprendizaje se cumplan.

Cabe destacar que, debido a los acuerdos de confidencialidad firmados con la organización huésped, la descripción detallada de procesos, entregables o casos específicos no podrá hacerse pública en este documento. En su lugar, se presentará la gestión y seguimiento del proyecto en términos generales, priorizando el desarrollo académico y profesional del alumno sin comprometer la información sensible de la empresa ni de sus clientes.

2.1 Administración del Proyecto

PROCESO	**Num. Aprox. Horas**
INICIO	6
PLANEACIÓN	8
EJECUCIÓN	30
SEGUIMIENTO Y CONTROL	20
CIERRE	10

2.2 Sustento Teórico y Metodológico

La empresa *IT Legal Services* se encuentra en una fase de creación, por lo que aún no existe un proceso metodológico formal establecido. La estrategia actual es iniciar con proyectos concretos (como el sistema de almacenamiento de alta disponibilidad), recopilar información real sobre los procesos internos y, posteriormente, seleccionar la metodología de gestión de proyectos más adecuada (Ágil, PMBOK, ITIL u otra) para el desarrollo del SOC.

2.3 Objetivos del Proyecto

Los principales objetivos del proyecto son:

1. Diseñar e implementar un **sistema de almacenamiento de alta disponibilidad**, que garantice la continuidad operativa de los servicios críticos de la empresa.
2. Establecer las bases tecnológicas para la futura creación de un **Centro de Operaciones de Seguridad (SOC)**.
3. Probar y validar la infraestructura para asegurar su resiliencia, redundancia y escalabilidad.
4. Documentar los procesos técnicos y operativos asociados al sistema de almacenamiento.
5. Transferir conocimiento al equipo de IT Legal Services para operación y soporte continuo.

EDT (Estructura de Desglose de Trabajo) a primer y segundo nivel

- Proyecto SOC (alcance mayor)
    - Fase 1: Sistema de almacenamiento de alta disponibilidad (**participación directa en este módulo**)
        - Diseño de arquitectura
        - Implementación de hardware/software
        - Pruebas de tolerancia a fallos
        - Documentación técnica
    - Fase 2: Monitoreo centralizado (futuro)
    - Fase 3: Integración de ciberseguridad avanzada (futuro)

2.4 Descripción del Proyecto

El proyecto PAP forma parte de un proyecto de mayor alcance: la creación de un **SOC en IT Legal Services**.
El sistema de almacenamiento de alta disponibilidad constituye la **primera etapa** de este plan estratégico, ya que proveerá la infraestructura necesaria para soportar los sistemas de monitoreo, análisis y respuesta que se desplegarán en fases posteriores.
Por tanto, las actividades desarrolladas no responden a un proceso repetitivo, sino que están enfocadas en **generar entregables estratégicos** que serán la base de proyectos futuros de ciberseguridad y monitoreo.

2.5 Plan de Trabajo

No.	Competencia	Nivel Adquirido al Inicio	Nivel Objetivo al final PAP	Objetivo final PAP	Prior
1	Conocimientos en almacenamiento de datos	1	3	3	A
2	Administración de sistemas Linux	1	3	3	A
3	Virtualización y contenedores (VMware, K8s)	0	2	2	M
4	Configuración de alta disponibilidad (HA)	0	2	2	A
5	Comunicación técnica en inglés	2	3	3	B
6	Documentación técnica y reportes	2	3	3	M

2.6 Equipo de Trabajo

Rol	Responsabilidad	Nombre (opcional)
Líder Técnico (1)	Definir lineamientos, validar arquitectura, aprobar entregables	-
Ingeniero de Infraestructura (1)	Configurar hardware, almacenamiento y sistemas de alta disponibilidad	-
Analista de Seguridad (1)	Evaluar implicaciones de seguridad, definir controles iniciales	-
Estudiante PAP (yo)	Implementación, documentación, pruebas de resiliencia, soporte en configuraciones	-

---

2.7 Plan de Comunicaciones

Emisor	Mensaje	Receptor	Medio	Frecuencia
Líder Técnico	Revisión de avances y feedback	Equipo del proyecto	Reuniones virtuales	Semanal
Estudiante PAP	Documentación de avances / entregables	Líder Técnico	Email / Docs	Semanal
Equipo	Resultados de pruebas	Todo el equipo	Reuniones / Chat	Ad-hoc

Emisor	Mensaje	Receptor	Medio	Frecuencia
Profesor PAP	Reportes de progreso académico	Profesor PAP	Plataforma PAP	Quincenal

---

2.8 Plan de Calidad

Emisor	Entregable	Receptor	Criterios	Siguiente paso
Estudiante PAP	Documentación de arquitectura	Líder Técnico	Claridad, precisión técnica, coherencia	Aprobación y almacenamiento
Ingeniero Infra	Configuración de almacenamiento HA	Líder Técnico	Redundancia validada, pruebas exitosas	Paso a pruebas de resiliencia
Analista Seguridad	Revisión de seguridad inicial	Líder Técnico	Cumplimiento de estándares básicos	Ajustes o validación final

---

2.9 Seguimiento y Control

El equipo realiza **reuniones semanales** con el líder del proyecto para revisar:

- Avances en la implementación.
- Resultados de pruebas de almacenamiento.
- Incidencias técnicas y acciones correctivas.
- Ajustes en el cronograma en caso de retrasos.

Además, con la **Coordinación PAP** y el **Profesor PAP** se efectúan reuniones de control académico en las que se entrega documentación, se reciben observaciones y se alinean las competencias educativas con los avances del proyecto.

2.10 Cierre del Proyecto

En el cierre de la fase del sistema de almacenamiento de alta disponibilidad, se realizó la **entrega de la arquitectura implementada y validada**.
El proceso de entrega-recepción incluyó la documentación, validación de pruebas de resiliencia y retroalimentación final del líder técnico.
Se cumplió con el **alcance, tiempo y calidad planeados**, sentando así las bases para continuar con las fases posteriores del proyecto SOC. Finalmente, se llevó a cabo una sesión de retroalimentación 1 a 1 con el líder técnico, donde se reconoció la aportación al proyecto y se dieron recomendaciones para continuar desarrollando competencias clave.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

Arquitectura de sistema de almacenamiento de alta disponibilidad - Diseño técnico implementado y validado
Documentación técnica del sistema - Manuales de operación y mantenimiento
Plan de controles ISO 27001 - Identificación y documentación de controles de seguridad aplicables
Reportes de pruebas de resiliencia - Validación de tolerancia a fallos del sistema

3.2 Estimación del Impacto

El sistema de almacenamiento establecerá las bases infraestructurales para el futuro SOC, beneficiando a la empresa con continuidad operativa y capacidad de respuesta ante incidentes. Los controles ISO 27001 documentados apoyarán procesos de certificación y cumplimiento normativo, fortaleciendo la posición competitiva de IT Legal Services. La documentación técnica facilitará la operación sostenible y la escalabilidad del proyecto, con impacto directo en la calidad de servicios de ciberseguridad ofrecidos a clientes de sectores críticos.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

Competencias técnicas desarrolladas:

- Diseño y configuración de sistemas de almacenamiento de alta disponibilidad
- Aplicación práctica de controles ISO 27001 en entornos reales
- Administración avanzada de sistemas Linux y virtualización

Competencias blandas:

- Comunicación técnica efectiva con líderes de proyecto
- Gestión del tiempo y priorización bajo confidencialidad
- Trabajo colaborativo en equipos multidisciplinarios

Descubrimientos del contexto: Comprendí la importancia crítica del cumplimiento normativo en ciberseguridad y cómo las regulaciones impactan directamente en las decisiones técnicas.

Saberes universitarios aplicados: Los conocimientos de redes, sistemas operativos y bases de datos fueron fundamentales, aunque noté necesidad de mayor formación en normativas internacionales.

Capacidad para proyectos futuros: Me considero capaz de participar activamente en proyectos de seguridad, y con preparación adicional, podría liderar implementaciones de ISO 27001.

4.2 Aprendizajes Sociales

Grupos beneficiados: Organizaciones que requieren protección de información sensible (sectores financiero, gobierno, manufactura, PYMES).

Bienes públicos generados: Fortalecimiento de capacidades nacionales en ciberseguridad y prevención de incidentes que afectan a la sociedad.

Apoyo a grupos sin recursos: Indirectamente, al proteger infraestructuras críticas, se contribuye a la estabilidad económica y social.

Contribución económica: Sí, fortaleciendo la competitividad de empresas mexicanas en ciberseguridad frente a amenazas globales.

Cambio de visión: Reconocí que la ciberseguridad no es solo técnica, sino un factor de protección social y económica fundamental.

Iniciativa de transformación: Participé en establecer bases tecnológicas que permitirán a la empresa escalar sus servicios y atender mejor a clientes.

4.3 Aprendizajes Éticos

Honestidad en entregables: La precisión técnica y transparencia en limitaciones fueron fundamentales, especialmente al manejar información confidencial.

Concordancia de valores: Encontré alineación entre mis valores de responsabilidad profesional y el compromiso ético de IT Legal Services con la protección de datos.

Conflictos éticos identificados: No identifiqué conflictos mayores, aunque reconocí la tensión entre eficiencia técnica y rigurosidad normativa.

Implicaciones de datos: La confidencialidad estricta reforzó mi comprensión sobre el manejo responsable de información sensible y consecuencias de filtraciones.

IA en ciberseguridad: Reflexioné sobre el uso ético de IA para detección de amenazas versus privacidad de usuarios.

Decisiones bajo incertidumbre: En configuraciones técnicas sin precedentes claros, prioricé la documentación exhaustiva y validación con supervisores antes de implementar.

Claridad profesional futura: Sí, ejerceré mi profesión priorizando la seguridad y privacidad de las personas, en organizaciones con valores éticos sólidos.

4.4 Aprendizajes Personales

Cambios en relaciones: Mayor empatía hacia responsabilidades laborales de otros y comunicación más asertiva.

Seguridad personal/profesional: Gané confianza en capacidades técnicas y en mi habilidad para aprender marcos normativos complejos.

Madurez adquirida: Sí, en gestión de responsabilidades, manejo de confidencialidad y profesionalismo bajo presión.

Autoconocimiento: Identifiqué fortalezas en resolución técnica y áreas de mejora en conocimientos regulatorios, confirmando mi interés en ciberseguridad.

Convivencia en diversidad: Aprendí a trabajar con profesionales de distintas especialidades, valorando perspectivas complementarias.

4.5 Tareas Aprendidas

Factores exitosos a repetir:

- Comunicación proactiva con el líder técnico
- Documentación detallada desde el inicio
- Solicitar retroalimentación temprana
- Respeto estricto a confidencialidad

Áreas de mejora identificadas:

- Mayor conocimiento previo en ISO 27001 habría acelerado resultados
- Gestión de tiempo en pruebas de resiliencia pudo optimizarse

  Necesidad de desarrollar más habilidades en inglés técnico

5. Conclusiones

La participación en este PAP representó una transición significativa del ámbito académico al profesional. La experiencia más inesperada fue comprender que la ciberseguridad efectiva requiere tanto rigor técnico como cumplimiento normativo, dos mundos que inicialmente percibía separados.

El reto de trabajar bajo estricta confidencialidad me enseñó el peso de la responsabilidad profesional más allá de las aulas. Establecer las bases de un SOC desde cero, aunque solo en su fase inicial, me mostró cómo proyectos estratégicos requieren visión a largo plazo y fundamentos sólidos.

El grado de satisfacción es alto: logré los objetivos planteados, desarrollé competencias críticas en áreas que identificaba como debilidades, y contribuí tangiblemente a un proyecto con impacto real. El esfuerzo exigido fue considerable, pero proporcional a los aprendizajes obtenidos.

Esta experiencia confirmó mi vocación en ciberseguridad y me preparó mejor para enfrentar los desafíos del campo profesional con una visión más integral y responsable.