|  | En esta pauta encontrarás preguntas orientadoras para tu reflexión. Las primeras te ayudarán a recordar las principales competencias aprendidas a lo largo de tu carrera. Las siguientes preguntas, buscan ayudarte a definir tu proyecto APT a partir de tus fortalezas, oportunidades de mejora e intereses profesionales.  Se sugiere que tengan como material de apoyo las evidencias recolectadas a lo largo de todo el proceso de portafolio, y que revises en el anexo de la guía del estudiante tu malla curricular, y las competencias y unidades de competencia por asignatura. |
| --- | --- |

| Puedes responder en cada una de las secciones por pregunta en esta guía. |
| --- |

| 1. Revisa la malla de tu carrera, piensa en las asignaturas o certificados de competencias que has cursado hasta ahora. Responde: |
| --- |
| ¿Cuáles son las asignaturas o certificados que más te gustaron y/o se relacionan con tus intereses profesionales? ¿Qué es lo que más te gustó de cada uno?   * **Certificación "PCAP - Programming Essentials In Python":** Esta fue una de mis primeras certificaciones que obtuve donde aprendí lo fundamental de Python, lo cual fue clave para la lógica que había que establecer en otras materias, dado que había que aplicar la misma estructura básica de programación. * **Certificaciones de Cisco y USACH:** Particularmente el "Junior Cybersecurity Analyst Career Path" y "Fundamentos de Seguridad en Redes". Lo que más me gustó fue la aplicación práctica de los conocimientos teóricos. No se trataba solo de aprender conceptos, sino de ponerlos en práctica, lo cual es fundamental en un área tan dinámica como la seguridad informática. * **Asignaturas de “Seguridad en sistemas”:** Aquí fue donde realmente conecté con mi pasión. Aprender a usar herramientas como Nmap, Metasploit y Burp Suite, y aplicarlas en entornos controlados proporcionados por el profesor, fue lo más atractivo. Me encantó el desafío mental de resolver problemas complejos y adoptar la mentalidad de un "hacker ético". * **Asignaturas de Integración de plataformas y desarrollo de aplicaciones móviles:** Disfruté mucho el poder aplicar estos conocimientos para construir proyectos full-stack como **RegisterApp**, donde pude desarrollar una solución completa desde cero y además descubrí como las diferentes herramientas y entornos dentro de internet se conectan y como se comunican. Me ayudo mucho en comprender su arquitectura y funcionamiento.   A partir de las certificaciones que obtienes a lo largo de la carrera ¿Existe valor en la o las certificaciones obtenidas? ¿Por qué?  Sí, estoy convencido de que las certificaciones que he obtenido tienen un gran valor por varias razones:   1. **Validan mis habilidades:** Demuestran de forma concreta que poseo conocimientos específicos en áreas críticas como ciberseguridad, redes y programación en Python, que son muy demandadas en la industria. 2. **Mejoran mi perfil profesional:** Siento que me diferencian de otros candidatos. Muestran mi compromiso con el aprendizaje continuo y mi especialización en un área que me apasiona. 3. **Son un estándar reconocido:** Las empresas confían en certificaciones como las de Cisco, lo que me da una ventaja al buscar oportunidades laborales, ya que garantizan un nivel de competencia técnica. |

| 2. Revisa las competencias y unidades de competencias correspondientes a cada asignatura de la malla de tu carrera. Marca en **verde** las competencias o unidades de competencia que consideras son tus **fortalezas** y en **rojo** las que requieren ser fortalecidas. A partir de este ejercicio responde: |
| --- |
| * ¿Cuáles consideras que tienes más desarrolladas y te sientes más seguro aplicando? ¿En cuáles te sientes más débil y requieren ser fortalecidas? * **Pensamiento innovador:** Haber obtenido el segundo lugar en el torneo "Innova Sostenible" de EY me confirmó que tengo la capacidad de crear soluciones creativas a problemas reales. * **Resolución de problemas y Pensamiento crítico:** Son habilidades que ejercito a diario en plataformas como HackTheBox. Analizar y explotar vulnerabilidades complejas como Shellshock o LFI me ha enseñado a pensar de forma metódica y fuera de lo común. * **Construir soluciones de software:** Me siento muy seguro en esta área, sobre todo al aplicar estándares de seguridad. Mi experiencia en pentesting y el desarrollo de mis propias aplicaciones me ha dado una base muy sólida. * **Capacidad de autogestión y Ética profesional:** Soy muy autónomo en mi aprendizaje, como lo demuestra mi actividad en plataformas de hacking. Además, entiendo que la ciberseguridad exige un estándar ético muy alto, el cual rige todas mis acciones. * **Administrar servicios y plataformas de TI:** Aunque tengo experiencia con Windows Server, reconozco que necesito fortalecer mis habilidades en la administración y, sobre todo, la seguridad de **plataformas en la nube (Cloud)** como AWS o Azure, ya que son el presente y futuro de la infraestructura de TI. * **Comunicación efectiva:** Me siento cómodo redactando informes técnicos para especialistas. Sin embargo, un área que debo potenciar es la habilidad de comunicar estos hallazgos a audiencias no técnicas, como gerentes o directivos, traduciendo el riesgo técnico a un impacto directo en el negocio. |

| 3. A partir de las respuestas anteriores y el perfil de egreso de tu carrera (competencias), responde las siguientes preguntas: |
| --- |
| * ¿Cuáles son tus principales intereses profesionales? ¿Hay alguna área de desempeño que te interese más?   Mi principal interés profesional es, sin lugar a dudas, la **ciberseguridad**. Específicamente, el área que más me apasiona es la **seguridad ofensiva y el pentesting**. Disfruto el reto de encontrar y explotar vulnerabilidades de manera ética para ayudar a las organizaciones a fortalecer sus defensas.   * ¿Cuáles son las principales competencias que se relacionan con tus intereses profesionales? ¿Hay alguna de ellas que sientas que requieres especialmente fortalecer?   Las competencias más importantes para mi área de interés son:   * **Construir soluciones de software** (para entender cómo se desarrollan y, por ende, cómo pueden fallar). * **Resolución de problemas** y **Pensamiento crítico** (esenciales para descubrir vulnerabilidades que no son obvias). * **Ética profesional** (la base del hacking ético).   Como mencioné antes, la competencia que siento que requiero fortalecer especialmente es la de **Administrar servicios y plataformas de TI**, pero con un enfoque en **Cloud Security**, para poder auditar y proteger infraestructuras modernas.   * ¿Cómo te gustaría que fuera tu escenario laboral en 5 años más? ¿Qué te gustaría estar haciendo?   En 5 años, me veo consolidado como un **Senior Penetration Tester** o un especialista en seguridad ofensiva. Mi objetivo es tener un dominio profundo en la auditoría de infraestructuras críticas y aplicaciones web complejas. Me gustaría estar trabajando en una empresa donde pueda enfrentar desafíos técnicos constantes, realizando pruebas de intrusión avanzadas y "Red Teaming" para simular ataques reales y ayudar a la organización a estar siempre un paso adelante de las amenazas. Más que gestionar, mi pasión está en la ejecución técnica, en encontrar esa vulnerabilidad que nadie más vio |

| 4. Finalmente, piensa en el proyecto que desarrollarás en APT y responde a las siguientes preguntas: |
| --- |
| * Los Proyectos APT que ya habías diseñado como plan de trabajo en el curso anterior, ¿se relacionan con tus proyecciones profesionales actuales? ¿cuál se relaciona más? ¿Requiere ajuste?   Mi proyecto APT, "Meetings APP", se alinea directamente con mis proyecciones profesionales. Mi rol asignado como **Especialista en Seguridad (CISO)** me brinda la oportunidad de aplicar mis conocimientos en un contexto práctico, abordando requisitos fundamentales como la **"Seguridad y Confidencialidad"**, la **"Autenticación"** y el **"Cifrado de Extremo a Extremo"**, que son pilares en mi área de interés.  Para potenciar aún más el valor de este proyecto y convertirlo en una pieza clave de mi portafolio, he decidido enfocarlo hacia mi área de especialización: la **Seguridad Ofensiva y el Pentesting**. Mi objetivo es realizar una **auditoría de seguridad completa (pentest)** a la aplicación una vez desarrollada. Este análisis incluirá la búsqueda de vulnerabilidades web comunes (OWASP Top 10), la revisión del código fuente y la ejecución de pruebas de intrusión.  Para darle un marco profesional, situaré el proyecto en el contexto de una **consultoría de seguridad externa**, donde actuaré como un pentester contratado para evaluar la aplicación antes de su lanzamiento al mercado. El entregable final será un **informe de pentesting profesional**, que detallará las vulnerabilidades encontradas, sus correspondientes pruebas de concepto (PoCs) y las recomendaciones técnicas para su mitigación. |