|  | 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 y, posteriormente, cargarla en la sección de reflexión de la Fase 1, para retroalimentación de tu docente. |
| --- |

| 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?**  El certificado de Seguridad Computacional ha sido mi favorito, ya que comprende asignaturas como Fundamentos de Ciberseguridad, Seguridad en Redes y Seguridad en Aplicaciones, que constituyen mi especialidad y el ámbito en el que deseo desarrollarme profesionalmente en el futuro. Me ha gustado especialmente trabajar en la detección de vulnerabilidades, el diseño de arquitecturas seguras y la implementación de medidas preventivas para proteger sistemas y datos críticos.  Además, disfruté obtener los siguientes certificados de módulo, cada uno aportando habilidades específicas:   * **Programación de Software**: Me permitió perfeccionar mi capacidad de construir aplicaciones seguras, aplicar buenas prácticas de codificación y crear soluciones confiables. * **Análisis y Desarrollo de Modelos de Datos**: Disfruté aprendiendo a organizar y resguardar datos de manera eficiente, asegurando integridad y disponibilidad en los sistemas. * **Arquitectura de Software**: Me gustó diseñar estructuras de sistemas escalables y seguras, capaces de resistir incidentes y ataques. * **Análisis y Planificación de Requerimientos Informáticos**: Me permitió comprender cómo identificar riesgos y definir requisitos de seguridad desde las primeras fases de un proyecto. * **Inteligencia de Negocios**: Aprendí a transformar datos en información útil, integrando además consideraciones de seguridad para la protección de la información. * **Internacional en Inglés Intermedio Alto**: Disfruté mejorar mis habilidades de comunicación en inglés, esenciales para comprender documentación técnica y colaborar en entornos internacionales de ciberseguridad. * **Gestión de Proyectos Informáticos**: Me gustó aprender a coordinar proyectos, aplicando metodologías que contemplen estándares de seguridad. * **Calidad de Software**: Me permitió entender la importancia de garantizar que los productos cumplan con estándares de seguridad y confiabilidad.   Cada certificado ha fortalecido mis competencias técnicas y transversales, integrando conocimientos que puedo aplicar en proyectos de seguridad informática y consolidando mi formación como especialista en Seguridad Computacional.  **A partir de las certificaciones que obtienes a lo largo de la carrera ¿Existe valor en la o las certificaciones obtenidas? ¿Por qué?**  Sí, las certificaciones obtenidas tienen gran valor, ya que validan habilidades específicas que se aplican en proyectos reales. Por ejemplo, las certificaciones en programación, análisis de datos y arquitectura de software refuerzan mi capacidad para diseñar sistemas seguros, mientras que las de gestión de proyectos e inglés facilitan la coordinación y comunicación en equipos multidisciplinarios. |

| 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?**  **Fortalezas:**   * Análisis y desarrollo de software con enfoque en seguridad. * Diseño de arquitecturas seguras y robustas. * Implementación de proyectos informáticos considerando riesgos y pruebas de certificación. * Gestión de proyectos con integración de protocolos de ciberseguridad. * Transformación de datos en información útil con resguardo de integridad y confidencialidad.   **Competencias a fortalecer:**   * Implementación avanzada de soluciones de ciberseguridad en entornos complejos. * Profundización en consultas y rutinas seguras en bases de datos. * Comunicación en inglés técnico, especialmente en contextos de ciberseguridad global.   En general, me siento sólida en los fundamentos técnicos y metodológicos, pero reconozco que necesito perfeccionar habilidades más avanzadas en defensa activa, respuesta a incidentes y comunicación especializada**.** |

| 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?**  Mis intereses profesionales se centran en la Seguridad Computacional, en áreas como la protección de infraestructuras críticas, la seguridad en redes, la gestión de vulnerabilidades, la auditoría de sistemas y la respuesta a incidentes. Me motiva trabajar en proyectos que permitan garantizar la integridad, disponibilidad y confidencialidad de los datos y sistemas de las organizaciones.  **¿Cuáles son las principales competencias que se relacionan con tus intereses profesionales? ¿Hay alguna de ellas que sientas que requieres especialmente fortalecer?**  **Competencias más relacionadas:**   * Desarrollo de software con estándares de seguridad. * Análisis y diseño de arquitecturas seguras. * Implementación de controles de seguridad en redes y aplicaciones. * Programación de rutinas seguras y soluciones integrales. * Gestión de proyectos de ciberseguridad.   **Competencias a reforzar:**   * Transformación y protección de grandes volúmenes de datos. * Gestión de proyectos de seguridad en escenarios internacionales. * Inglés técnico aplicado a la seguridad computacional.   **¿Cómo te gustaría que fuera tu escenario laboral en 5 años más? ¿Qué te gustaría estar haciendo?**  Me visualizo como especialista en Seguridad Computacional, formando parte de un equipo de ciberseguridad o liderando proyectos de protección digital en una organización. Me gustaría estar trabajando en la detección de amenazas, gestión de vulnerabilidades y diseño de sistemas seguros que protejan información crítica. Además, deseo estar certificado en estándares internacionales de seguridad (como CISSP, CEH o ISO 27001) y consolidar mi rol estratégico en proyectos de ciberdefensa. |

| 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?**  Sí, el proyecto JobFlex – Plataforma de Empleo Multiperfil se relaciona directamente con mis proyecciones profesionales, ya que integra aspectos de seguridad informática en el desarrollo de software, la gestión de usuarios y la protección de datos. Este proyecto me permite aplicar competencias en programación, arquitectura de software segura, gestión de bases de datos y medidas de seguridad en aplicaciones web, todas alineadas con mi interés en seguridad computacional.  El proyecto no requiere ajustes significativos, pero podría reforzarse agregando capas de ciberseguridad, como autenticación multifactor, cifrado de datos y monitoreo de accesos, lo que aumentaría su valor como experiencia profesional y práctica en mi formación como especialista en seguridad.  **Si no hay ninguna que se relacione suficiente:**  **¿Qué área(s) de desempeño y competencias debería abordar este Proyecto APT?**  El Proyecto APT debería abordar principalmente el área de Seguridad Computacional, con foco en competencias como:   * Detección y gestión de vulnerabilidades en aplicaciones y redes. * Implementación de medidas de protección en entornos digitales. * Diseño de arquitecturas seguras y robustas para sistemas de información. * Integración de protocolos de seguridad en bases de datos y plataformas web. * Respuesta a incidentes y manejo de riesgos tecnológicos.   Estas competencias permitirían aplicar directamente los conocimientos adquiridos en mi formación y reforzar las habilidades necesarias para mi desarrollo profesional.  **¿Qué tipo de proyecto podría ayudarte más en tu desarrollo profesional?**  El tipo de proyecto que más contribuiría a mi desarrollo profesional sería uno orientado a la seguridad de aplicaciones web o de infraestructuras críticas, por ejemplo:   * El diseño de un sistema con autenticación multifactor y cifrado de datos. * El desarrollo de un módulo de auditoría y monitoreo de accesos en tiempo real. * La implementación de una plataforma con análisis de vulnerabilidades automatizado.   Un proyecto de este estilo no solo consolidaría mis conocimientos técnicos, sino que también me permitiría practicar buenas prácticas de ciberseguridad en un entorno cercano a la realidad profesional.  **¿En qué contexto se debería situar este Proyecto APT?**  El contexto más adecuado sería un entorno organizacional, simulando la protección de datos e infraestructura de una empresa u organismo público. De esta forma, el proyecto tendría un enfoque práctico y aplicable, ya que permitiría trabajar con escenarios de seguridad reales como:   * Protección de información sensible de clientes o empleados. * Cumplimiento de normativas y estándares de seguridad (ISO 27001, GDPR, etc.). * Respuesta a intentos de intrusión o ciberataques simulados.   Situar el proyecto en este tipo de contexto favorecería el desarrollo de soluciones realistas, directamente relacionadas con los desafíos que enfrentan actualmente las organizaciones en el ámbito de la ciberseguridad. |