SALTA, 10-MAR-2026

RESOLUCIÓN Nº 149
UNIVERSIDAD PROVINCIAL DE LA ADMINISTRACIÓN, TECNOLOGÍA Y OFICIOS
Expediente SICAD N° 258/26

VISTO el Artículo 75, apartado 19, de la Constitución Nacional, la Ley nacional 24521 y la Ley 8312, modificatoria de su similar 7803, y

CONSIDERANDO:

Que, de conformidad con lo dispuesto por el Artículo 26 de la Ley 24521, la enseñanza superior universitaria estará a cargo de las Universidades Nacionales, de las Universidades Provinciales y Privadas, y de los Institutos Universitarios;

Que mediante Ley 8312, modificatoria de su similar 7803, se crea la Universidad Provincial de la Administración, Tecnología y Oficios (UPATecO) como persona jurídica pública, con autonomía institucional y académica, y autarquía financiera y administrativa;

Que, por su parte, el Artículo 27 de la Ley 7803, modificado por Ley 8312, establece que los títulos que emita la UPATecO tendrán validez en todo el territorio de la provincia de Salta y habilitarán a los egresados a ejercer su profesión u oficio, conforme la normativa vigente en la materia;

Que, en las actuaciones de referencia, la Secretaría Académica de esta Universidad eleva el Proyecto de Plan de Estudios correspondiente a la carrera de pregrado “Tecnicatura Universitaria en Ciberseguridad y Protección de Sistemas Digitales”;

Que dicha carrera se organiza en base al Modelo de Formación Modular y Certificación por Competencias, con módulos que conforman unidades académicas mínimas;

Que la carrera mencionada tiene como objetivos, entre otros, la formación de técnicos universitarios con una sólida base científica, tecnológica y práctica, capaces de prevenir, detectar, analizar y mitigar amenazas informáticas, proteger infraestructuras tecnológicas y gestionar la seguridad de la información, contribuyendo a la resiliencia digital, la protección de datos y el desarrollo tecnológico, en el marco de estándares de calidad, normativa vigente y ética profesional;

Que en autos queda claramente establecida la fundamentación de la necesidad de la carrera, duración, perfil del egresado, requisitos de ingreso, objetivos de la carrera, metodología, evaluación, organización curricular, contenidos mínimos de cada espacio curricular, entre otros ítems;

.. //

.. // RESOLUCIÓN Nº 149
Expediente SICAD N° 258/26

Que la Dirección Jurídica de esta Universidad se expide favorablemente a través de Dictamen N° 159/26, por lo que corresponde el dictado del acto administrativo pertinente, en virtud de la Ley 8312, modificatoria de su similar 7803, y del Decreto N° 88/23;

Por ello;

EL RECTOR DE LA UNIVERSIDAD PROVINCIAL
DE LA ADMINISTRACIÓN, TECNOLOGÍA Y OFICIOS

R E S U E L V E :

ARTÍCULO 1º.- Aprobar el Plan de Estudios de la carrera de pregrado “Tecnicatura Universitaria en Ciberseguridad y Protección de Sistemas Digitales”, de la Universidad Provincial de la Administración, Tecnología y Oficios (UPATecO), que como Anexo forma parte de este instrumento legal.

ARTÍCULO 2°.- La presente resolución será refrendada por la señora Vicerrectora de esta Universidad.

ARTÍCULO 3°.- Comunicar y archivar.

Firmado digitalmente por
Dra. MARÍA de los D. TALENS
Vicerrectora UPATecO

Firmado digitalmente por
Dr. CARLOS MORELLO
Rector UPATecO

RC
DD

UNIVERSIDAD PROVINCIAL DE ADMINISTRACIÓN,

TECNOLOGÍA Y OFICIOS (UPATecO)

AUTORIDADES

RECTOR
Dr. Carlos Morello

VICERRECTORA

Dr. María de los D. Talens

PLAN DE ESTUDIO 2026

IDENTIFICACIÓN DE LA CARRERA

1.- CARACTERÍSTICAS DE LA CARRERA

Denominación de la Carrera:	**Tecnicatura Universitaria en Ciberseguridad y Protección de Sistemas Digitales**
Nivel Académico:	**Tecnicatura Universitaria**
Modalidad:	**Híbrida**
Título que Otorga	**Técnico Universitario en Ciberseguridad y Protección de Sistemas Digitales**
Duración de la carrera:	**2 años y medio**
Régimen de cursado:	**Cuatrimestral**
Carga Horaria Total:	**1600 horas reloj**

2.- FUNDAMENTACIÓN:

2.1.- Contexto y pertinencia de la propuesta

La acelerada digitalización de los sectores productivos, gubernamentales, financieros, educativos, sanitarios e industriales ha incrementado de manera exponencial la dependencia de infraestructuras tecnológicas, redes de comunicación y sistemas digitales. Este proceso ha traído consigo un crecimiento sostenido de amenazas informáticas, ataques cibernéticos, vulnerabilidades en sistemas y riesgos asociados a la protección de datos, lo que posiciona a la ciberseguridad como un área estratégica para la estabilidad institucional, la competitividad económica y la soberanía tecnológica.

En el contexto actual, las organizaciones públicas y privadas requieren profesionales técnicos capacitados para prevenir, detectar y mitigar incidentes de seguridad informática, proteger infraestructuras críticas y garantizar la integridad, confidencialidad y disponibilidad de la información. Sin embargo, existe una marcada brecha entre la creciente demanda de perfiles especializados en ciberseguridad y la oferta formativa técnica universitaria orientada específicamente a la protección de sistemas digitales.

La Tecnicatura Universitaria en Ciberseguridad y Protección de Sistemas Digitales se propone responder a esta necesidad, ofreciendo una formación tecnológica, práctica y orientada a la resolución de problemáticas reales vinculadas a la seguridad de redes, sistemas, aplicaciones y datos, contribuyendo a la profesionalización del sector y a la reducción del riesgo digital en el ámbito regional y nacional.

2.2.- Vinculación con la misión institucional

La propuesta se alinea con la misión institucional de formar recursos humanos altamente capacitados en áreas tecnológicas estratégicas, promoviendo la innovación, la empleabilidad y el desarrollo productivo basado en el conocimiento.

La tecnicatura fortalece la articulación entre el sistema universitario y el ecosistema tecnológico regional, acompañando la expansión de la economía digital y la demanda de perfiles técnicos especializados en seguridad informática. Asimismo, contribuye a la consolidación de capacidades locales para la protección de infraestructuras digitales en organismos públicos, empresas privadas y emprendimientos tecnológicos.

De esta manera, la carrera promueve la inserción laboral temprana en sectores vinculados a tecnologías de la información, servicios digitales, telecomunicaciones, desarrollo de software y gestión de datos, consolidando un perfil técnico con alto impacto estratégico.

2.3.- Fundamentación académica y formativa

La estructura curricular se organiza de manera progresiva e integrada, articulando campos formativos que garantizan una sólida base técnica y profesional:

- Fundamentos de informática, redes y sistemas operativos.
- Programación y arquitectura de sistemas digitales.
- Seguridad informática, análisis de vulnerabilidades y gestión de incidentes.
- Protección de datos, criptografía y normativas de ciberseguridad.

La formación combina conocimientos teóricos sólidos en redes, protocolos de comunicación, arquitectura de sistemas, bases de datos y fundamentos de programación, con competencias técnicas orientadas a la identificación de amenazas, implementación de medidas preventivas, análisis forense digital, pruebas de penetración y gestión de riesgos.

Asimismo, se incorporan contenidos vinculados a ética digital, protección de datos personales, normativa nacional e internacional en materia de seguridad informática y uso responsable de tecnologías, asegurando una formación integral y comprometida con la legalidad y la responsabilidad profesional.

Las prácticas profesionalizantes permiten aplicar los conocimientos en entornos reales o simulados, mediante laboratorios de seguridad, simulación de ataques controlados, análisis de incidentes y diseño de políticas de protección, fortaleciendo la capacidad de trabajo en equipos técnicos interdisciplinarios y la resolución de problemas complejos.

2.4.- Contribución al desarrollo regional y sectorial

La implementación de esta tecnicatura contribuye al fortalecimiento del ecosistema digital regional, impulsando la generación de capacidades locales para la protección de sistemas informáticos en organismos públicos, empresas, pymes y emprendimientos tecnológicos.

La formación de técnicos universitarios especializados en ciberseguridad promueve la creación de empleo calificado, el desarrollo de servicios tecnológicos especializados y la consolidación de un entorno digital más seguro y resiliente. Asimismo, favorece la protección de

infraestructuras críticas, la defensa ante amenazas cibernéticas y la reducción de vulnerabilidades en sectores estratégicos.

De este modo, la Tecnicatura Universitaria en Ciberseguridad y Protección de Sistemas Digitales se posiciona como una respuesta formativa pertinente frente a los desafíos de la transformación digital, contribuyendo al desarrollo productivo, la seguridad tecnológica y la soberanía digital del territorio.

3.- OBJETIVOS DE LA CARRERA

Objetivo General

Formar técnicos universitarios en Ciberseguridad y Protección de Sistemas Digitales con una sólida base científica, tecnológica y práctica, capaces de prevenir, detectar, analizar y mitigar amenazas informáticas, proteger infraestructuras tecnológicas y gestionar la seguridad de la información, contribuyendo a la resiliencia digital, la protección de datos y el desarrollo tecnológico, en el marco de estándares de calidad, normativa vigente y ética profesional.

1. **Objetivos Específicos**
2. La carrera tiene como objetivos específicos:
3. Proporcionar una formación científica y tecnológica que permita comprender los fundamentos de redes, sistemas operativos, arquitectura de sistemas, protocolos de comunicación y principios de seguridad informática.
4. Desarrollar competencias técnicas para la identificación y análisis de vulnerabilidades en sistemas, redes y aplicaciones, aplicando metodologías y herramientas actuales de evaluación y monitoreo de seguridad.
5. Formar en la implementación de mecanismos de protección, incluyendo configuración segura de redes, gestión de accesos, cifrado de datos, políticas de seguridad y controles preventivos.
6. Formar en la detección y gestión de incidentes de seguridad informática, incluyendo monitoreo, respuesta ante incidentes, análisis forense digital básico y recuperación de sistemas.
7. Promover la aplicación de buenas prácticas en gestión de riesgos, continuidad del negocio y protección de infraestructuras críticas, en conformidad con estándares y normativas nacionales e internacionales.

8. Fomentar el análisis crítico del impacto social, ético y legal de la ciberseguridad, promoviendo la protección de datos personales, la privacidad digital y el uso responsable de tecnologías.
9. Favorecer el desarrollo de habilidades de comunicación técnica, trabajo colaborativo y adaptación a entornos tecnológicos dinámicos, interdisciplinarios y de alta exigencia.
10. Formar a los estudiantes para su inserción profesional mediante prácticas profesionalizantes progresivas y proyectos integradores aplicados a entornos reales o simulados de seguridad informática.
11. Contribuir a la formación de recursos humanos calificados que fortalezcan el ecosistema tecnológico regional, apoyando la protección de infraestructuras digitales en sectores públicos y privados y el desarrollo de la economía del conocimiento.

4.- PERFIL DEL EGRESADO

El egresado de la Tecnicatura Universitaria en Ciberseguridad y Protección de Sistemas Digitales será un técnico universitario con sólida formación en informática, redes, arquitectura de sistemas y seguridad de la información, capacitado para participar en la prevención, detección y mitigación de amenazas digitales en entornos organizacionales. Estará preparado para colaborar en el diseño, implementación y mantenimiento de políticas y soluciones de seguridad informática que garanticen la integridad, confidencialidad y disponibilidad de la información.

Contará con competencias técnicas para analizar vulnerabilidades en sistemas, redes y aplicaciones, configurar infraestructuras seguras, implementar mecanismos de control de acceso y cifrado, monitorear eventos de seguridad y participar en la gestión de incidentes informáticos. Podrá integrarse a equipos interdisciplinarios en áreas de tecnología, soporte técnico, administración de redes y seguridad informática, contribuyendo a la protección de activos digitales y a la reducción de riesgos en organizaciones públicas y privadas.

Asimismo, poseerá una formación ética y crítica que le permitirá actuar con responsabilidad en la gestión de información sensible, el tratamiento de datos personales y la aplicación de tecnologías de seguridad, considerando aspectos legales, normativos y de privacidad. Su desempeño estará orientado por principios de profesionalismo, confidencialidad y compromiso con la seguridad digital, contribuyendo al fortalecimiento de entornos tecnológicos seguros y resilientes.

5.- COMPETENCIAS DEL EGRESADO

El egresado estará capacitado para desarrollar las siguientes competencias:

a) Competencias técnicas y operativas

- Configurar y administrar sistemas operativos y redes con criterios de seguridad.
- Identificar, analizar y evaluar vulnerabilidades en sistemas, aplicaciones y redes informáticas.
- Implementar mecanismos de protección como control de accesos, autenticación, cifrado y políticas de seguridad.
- Monitorear eventos de seguridad y participar en la detección y respuesta ante incidentes informáticos.
- Aplicar herramientas básicas de análisis de tráfico, pruebas de penetración y evaluación de seguridad.
- Colaborar en la implementación de planes de continuidad operativa y recuperación ante desastres.
- Realizar tareas básicas de análisis forense digital en entornos controlados.
- Gestionar configuraciones seguras en entornos locales y plataformas cloud.

b) Competencias en gestión tecnológica y buenas prácticas

- Aplicar principios de gestión de riesgos en seguridad informática.
- Implementar políticas y procedimientos de seguridad de la información en organizaciones.
- Documentar configuraciones, incidentes y procesos técnicos de manera sistemática.
- Aplicar estándares y normativas de ciberseguridad nacionales e internacionales.
- Gestionar controles de acceso y administración de usuarios con criterios de trazabilidad y auditoría.
- Integrar prácticas de seguridad en proyectos tecnológicos y entornos colaborativos.
- Interpretar requerimientos organizacionales y traducirlos en soluciones técnicas de protección digital.

c) Competencias éticas y transversales

- Actuar con responsabilidad profesional en la gestión de información sensible y datos personales.
- Respetar principios de confidencialidad, integridad y disponibilidad de la información.

- Analizar críticamente el impacto social, legal y organizacional de las decisiones en materia de seguridad digital.
- Integrarse a equipos interdisciplinarios de tecnología, soporte y gestión.
- Comunicar incidentes, diagnósticos y recomendaciones técnicas de manera clara, oral y escrita.
- Adaptarse a la evolución permanente de las amenazas y tecnologías mediante actualización y aprendizaje continuo.

6.- ALCANCES DEL TÍTULO

El título de **Técnico Universitario en Ciberseguridad y Protección de Sistemas Digitales** habilita al egresado a desempeñarse en ámbitos públicos y privados vinculados a la prevención, protección y gestión de la seguridad de la información y de infraestructuras tecnológicas, en tareas de apoyo técnico, operativo y de gestión en ciberseguridad, bajo la supervisión de profesionales responsables cuando la complejidad del proyecto o la normativa vigente así lo requiera.

En particular, el egresado estará habilitado para:

1. Participar en la identificación y evaluación de vulnerabilidades en sistemas, redes y aplicaciones informáticas.
2. Implementar configuraciones seguras en sistemas operativos, redes y dispositivos, aplicando buenas prácticas de seguridad informática.
3. Colaborar en la instalación y administración de herramientas de monitoreo, detección de intrusiones y análisis de eventos de seguridad.
4. Participar en la gestión y respuesta inicial ante incidentes de seguridad informática, aplicando protocolos establecidos y colaborando en procesos de recuperación.
5. Implementar mecanismos básicos de protección como control de accesos, autenticación segura, cifrado de información y respaldo de datos.
6. Colaborar en la elaboración e implementación de políticas y procedimientos de seguridad de la información en organizaciones públicas y privadas.
7. Participar en tareas de análisis forense digital básico en entornos controlados, respetando protocolos técnicos y legales.
8. Aplicar normativas vigentes en materia de protección de datos personales, privacidad y seguridad de la información.

9. Elaborar informes técnicos, registros de incidentes y documentación de seguridad para su comunicación a equipos interdisciplinarios y áreas de gestión.
10. Integrar equipos de trabajo en áreas de tecnología, soporte técnico, administración de redes y seguridad informática en empresas, organismos públicos, consultoras tecnológicas, proveedores de servicios digitales o emprendimientos propios vinculados a la economía del conocimiento.

Las actividades mencionadas se desarrollarán sin perjuicio de las incumbencias propias de los profesionales universitarios de grado en ingeniería, informática, ciencias de la computación u otras disciplinas afines, quienes asumirán la responsabilidad técnica integral de los proyectos cuando corresponda, conforme a la normativa vigente.

7.- REQUISITOS DE INGRESO

Podrán cursar esta tecnicatura universitaria aquellas personas que:

• Posean título secundario o equivalente completo, cualquiera sea su modalidad, emitidos por instituciones de gestión estatal o privada y consten con el debido reconocimiento ministerial, conforme lo establece el artículo 7º de la Ley de Educación Superior Nº 24521.

• Quienes no posean título secundario o equivalente, pero que sean mayores de 25 años y se encuentren en el marco de excepcionalidad establecido en la segunda parte del artículo 7º de la Ley de Educación Superior Nº 24521.

• Acrediten título secundario completo, emitido por otro país, pero debidamente reconocido por el Ministerio de Relaciones Exteriores y Culto y el Ministerio de Educación de la Nación.

• Registren su preinscripción en las fechas establecidas según resolución rectoral.

8.- PLAN DE ESTUDIOS Y ESTRUCTURA CURRICULAR

COD	MÓDULO	RÉGIMEN	CARGA HORARIA SEMANAL	CARGA HORARIA TOTAL	CORRELA-TIVAS PARA CERTIFICAR	CAMPO DE FORMACIÓN
PRIMER AÑO (1° CUATRIMESTRE)						
1	Alfabetización Académica y Comunicación Técnica	cuatrimestral	4	64	-	General

2	Matemática Aplicada a la Computación	cuatrimestral	5	80	-	Fundamentos
3	Introducción a la Informática y Arquitectura de Sistemas	cuatrimestral	5	80	-	Fundamentos
4	Práctica Profesional I: Laboratorio de Sistemas Operativos	cuatrimestral	5	80	-	Práctica
PRIMER AÑO (2° CUATRIMESTRE)						
5	Inglés Técnico I	cuatrimestral	4	64	-	General
6	Redes y Protocolos de Comunicación	cuatrimestral	4	64	3	Específica
7	Programación para Seguridad Informática	cuatrimestral	5	80	2	Específica
8	Práctica Profesional II: Configuración y Administración de Redes	cuatrimestral	5	80	4	Práctica
SEGUNDO AÑO (1° CUATRIMESTRE)						
9	Legislación Informática y Protección de Datos	cuatrimestral	4	64	-	General
10	Fundamentos de Ciberseguridad	cuatrimestral	4	64	6-7	Específica
11	Criptografía y Seguridad de la Información	cuatrimestral	6	96	2	Específica
12	Práctica Profesional III: Análisis de Vulnerabilidades	cuatrimestral	6	96	8	Práctica
SEGUNDO AÑO (2° CUATRIMESTRE)						
13	Gestión de Riesgos y Seguridad Organizacional	cuatrimestral	6	96	10	Específica
14	Seguridad en Sistemas y Aplicaciones	cuatrimestral	6	96	7-10	Específica
15	Ética y Responsabilidad Profesional en Entornos Digitales	cuatrimestral	4	64	-	General
16	Ingles técnico II	cuatrimestral	4	64	5	General
17	Práctica Profesional IV: Gestión de Incidentes y Monitoreo	cuatrimestral	5	80	12	Práctica
TERCER AÑO (1° CUATRIMESTRE)						
18	Seguridad en Entornos Cloud e Infraestructuras Críticas	cuatrimestral	6	96	13-14	Específica
19	Auditoría y Normativas de Seguridad Informática	cuatrimestral	4	64	9-13	Específica
20	Liderazgo, Comunicación y Trabajo en Equipos Tecnológicos	cuatrimestral	3	48	-	General
21	Práctica Profesional V – Proyecto Final Integrador	cuatrimestral	5	80	17	Práctica

9.- Contenidos Mínimos y Bibliografía Sugerida

1 - Alfabetización Académica y Comunicación Técnica

La alfabetización académica como proceso de ingreso a la cultura universitaria. Lectura y escritura en contextos académicos y técnico-profesionales. Diferencias entre textos de divulgación, textos académicos y textos técnicos vinculados a la minería, el ambiente y el muestreo.
Estrategias de lectura comprensiva. Identificación de ideas principales y secundarias. Reconocimiento de la estructura de textos expositivos y argumentativos. Uso de paratextos: títulos, subtítulos, gráficos, tablas y referencias. Interpretación crítica de información técnica y científica.
Comprensión de textos técnicos y normativos. Lectura de protocolos, manuales, normas técnicas y procedimientos operativos vinculados al muestreo y control de calidad. Vocabulario técnico específico del campo minero y ambiental. Uso de glosarios y fuentes especializadas.
Producción de textos académicos y técnicos. Escritura de resúmenes, informes técnicos de muestreo y registros de campo. Organización lógica del texto. Coherencia y cohesión. Uso adecuado del lenguaje técnico. Normas básicas de citación y referencias bibliográficas. Introducción a las normas APA.
Comunicación oral en contextos académicos y laborales. Exposición de trabajos prácticos. Presentación de informes y resultados. Comunicación efectiva en equipos técnicos. Ética académica, honestidad intelectual y prevención del plagio.

Bibliografía sugerida

- Carlino, P. (2013). *Alfabetización académica: Leer y escribir en la universidad*. Fondo de Cultura Económica.
- Cassany, D. (2006). *Tras las líneas: Sobre la lectura contemporánea*. Anagrama.
- Eco, U. (2014). *Cómo se hace una tesis* (reimp.). Gedisa.
- Hernández Sampieri, R., Fernández Collado, C., & Baptista, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill.
- Swales, J. M., & Feak, C. B. (2012). *Academic writing for graduate students* (3rd ed.). University of Michigan Press.

2 - Matemática Aplicada a la Computación

Lógica matemática y razonamiento formal, proposiciones y conectores lógicos, tablas de verdad, cuantificadores y equivalencias lógicas, conjuntos y relaciones, funciones y tipos de funciones, nociones de combinatoria básica, álgebra lineal aplicada a la computación, vectores y matrices, operaciones matriciales, sistemas de ecuaciones lineales, espacios vectoriales, nociones de transformaciones lineales, fundamentos de cálculo diferencial, funciones reales de una variable, límites y derivadas, interpretación geométrica de la derivada, optimización básica de funciones, introducción al cálculo en varias variables, conceptos fundamentales de probabilidad, variables aleatorias discretas, esperanza matemática y varianza, nociones de estadística descriptiva, interpretación matemática de algoritmos, complejidad básica y crecimiento de funciones, aplicación de herramientas matemáticas en problemas computacionales.

- **Bibliografía sugerida**

- Rosen, K. H. (2019). *Discrete mathematics and its applications* (8th ed.). McGraw-Hill Education.
- Lay, D. C., Lay, S. R., & McDonald, J. J. (2016). *Linear algebra and its applications* (5th ed.). Pearson.
- Stewart, J. (2016). *Calculus: Early transcendentals* (8th ed.). Cengage Learning.

- Grimaldi, R. P. (2004). *Discrete and combinatorial mathematics: An applied introduction* (5th ed.).
- Pearson. Blitzstein, J. K., & Hwang, J. (2019). *Introduction to probability* (2nd ed.). Chapman & Hall/CRC.

3 - Introducción a la Informática y Arquitectura de Sistemas

Conceptos fundamentales de informática, evolución histórica de la computación, representación digital de la información, sistemas de numeración (binario, decimal, hexadecimal), codificación de datos y unidades de almacenamiento, estructura y funcionamiento de una computadora, arquitectura de von Neumann y arquitecturas modernas, componentes de hardware (CPU, memoria, dispositivos de almacenamiento y periféricos), funcionamiento básico del procesador, ciclos de instrucción, sistemas operativos y su rol en la gestión de recursos, procesos e hilos de ejecución, memoria y almacenamiento, fundamentos de redes informáticas, modelos cliente-servidor y arquitectura distribuida, virtualización y nociones de computación en la nube, seguridad básica en sistemas informáticos, conceptos de software, tipos de software y ciclo de vida básico de desarrollo, introducción a la lógica computacional y estructura de programas, nociones iniciales de ciberseguridad asociadas a la arquitectura de sistemas.

Bibliografía sugerida

- Tanenbaum, A. S., & Austin, T. (2013). *Structured computer organization* (6th ed.). Pearson.
- Stallings, W. (2019). *Computer organization and architecture: Designing for performance* (11th ed.). Pearson.
- Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). *Operating system concepts* (10th ed.). Wiley.
- Forouzan, B. A. (2017). *Data communications and networking* (5th ed.). McGraw-Hill Education.
- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5th ed.). Pearson.

4 - Práctica Profesional I: Laboratorio de Sistemas Operativos

Instalación y configuración de sistemas operativos Windows y Linux en entornos físicos y virtualizados, gestión de usuarios y permisos, administración básica de procesos y servicios, manejo de sistemas de archivos, particionado y montaje de unidades de almacenamiento, configuración de redes locales en sistemas operativos, administración de recursos del sistema (CPU, memoria y almacenamiento), uso de línea de comandos en entornos Linux y PowerShell en Windows, configuración de políticas básicas de seguridad, gestión de actualizaciones y parches, monitoreo de rendimiento del sistema, análisis de registros (logs) del sistema operativo, identificación de vulnerabilidades básicas en configuraciones inseguras, implementación de medidas de hardening inicial, creación y gestión de máquinas virtuales, prácticas de respaldo y restauración de sistemas, simulación de incidentes básicos y recuperación del sistema, documentación técnica de configuraciones realizadas.

Bibliografía sugerida

- Nemeth, E., Snyder, G., Hein, T. R., & Whaley, B. (2017). *UNIX and Linux system administration handbook* (5th ed.). Pearson.
- Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). *Operating system concepts* (10th ed.). Wiley.
- Shotts, W. E. (2019). *The Linux command line* (2nd ed.). No Starch Press.

- Russinovich, M., Solomon, D., & Ionescu, A. (2017). *Windows internals* (7th ed.). Microsoft Press.
- Nakamura, E., & Nakamura, L. (2020). *Linux hardening in hostile networks*. Apress.

5 - Inglés Técnico I

Fundamentos de comprensión lectora en inglés aplicado a tecnologías de la información y ciberseguridad, vocabulario técnico específico de informática, redes y seguridad digital, estructuras gramaticales básicas para lectura e interpretación de textos técnicos, análisis de manuales, documentación técnica y artículos especializados, comprensión de especificaciones técnicas y estándares internacionales, lectura e interpretación de normativas y reportes de seguridad, terminología relacionada con sistemas operativos, redes, criptografía y gestión de incidentes, redacción básica de informes técnicos en inglés, elaboración de correos y comunicaciones formales en entornos tecnológicos, comprensión auditiva de presentaciones técnicas y conferencias especializadas, uso de glosarios técnicos y herramientas de traducción asistida, análisis de casos prácticos mediante documentación original en inglés, desarrollo de habilidades para interpretar documentación de fabricantes y proveedores tecnológicos, fortalecimiento de la autonomía en la lectura de fuentes académicas y técnicas en idioma inglés.

Bibliografía sugerida

- Glendinning, E. H., & McEwan, J. (2013). *Oxford English for information technology* (2nd ed.). Oxford University Press.
- Hewings, M. (2013). *Advanced grammar in use* (3rd ed.). Cambridge University Press.
- Murphy, R. (2019). *English grammar in use* (5th ed.). Cambridge University Press.
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. NIST.
- Stallings, W. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.

6 - Redes y Protocolos de Comunicación

Fundamentos de redes informáticas, tipos de redes (LAN, WAN, MAN, WLAN), topologías físicas y lógicas, modelo OSI y modelo TCP/IP, funciones y características de cada capa, direccionamiento IP (IPv4 e introducción a IPv6), máscaras de subred y subnetting básico, protocolos de comunicación (TCP, UDP, ICMP), resolución de nombres (DNS), protocolo DHCP, protocolos de aplicación (HTTP, HTTPS, FTP, SMTP, POP3, IMAP), dispositivos de red (switches, routers, firewalls), configuración básica de redes cableadas e inalámbricas, fundamentos de routing y switching, redes privadas virtuales (VPN), introducción a redes seguras, conceptos de cifrado en tránsito (SSL/TLS), análisis básico de tráfico de red, herramientas de diagnóstico y monitoreo (ping, traceroute, netstat, Wireshark), identificación de vulnerabilidades en redes, fundamentos de segmentación de red y buenas prácticas de seguridad en infraestructura de comunicaciones.

Bibliografía sugerida

- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5th ed.). Pearson.
- Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.
- Stallings, W. (2020). *Data and computer communications* (10th ed.). Pearson.
- Odom, W. (2020). *CCNA 200-301 official cert guide* (Vols. 1–2). Cisco Press.
- Scarfone, K., & Hoffman, P. (2016). *Guide to enterprise network security* (NIST Special Publication 800-41). National Institute of Standards and Technology.

7 - Programación para Seguridad Informática

Fundamentos de programación orientada a la seguridad, sintaxis y estructuras básicas en un lenguaje aplicado a ciberseguridad (Python u otro lenguaje equivalente), estructuras de control, funciones y modularización, manejo de archivos y procesamiento de datos, manipulación de cadenas y expresiones regulares, programación orientada a objetos aplicada a herramientas de seguridad, uso de librerías para automatización de tareas de red, creación de scripts para escaneo y monitoreo básico, introducción al análisis de vulnerabilidades mediante scripting, interacción con APIs y servicios web, consumo y análisis de datos en formato JSON y XML, automatización de pruebas básicas de seguridad, manejo de sockets y comunicación en red desde código, fundamentos de criptografía aplicada en programación (hashing, cifrado simétrico básico), validación de entradas y prevención de vulnerabilidades comunes (inyecciones, manejo inseguro de datos), registro y manejo de logs, desarrollo de herramientas simples para análisis de tráfico o revisión de configuraciones, buenas prácticas de programación segura y documentación técnica del código desarrollado.

Bibliografía sugerida

- Seitz, J. (2021). *Black hat Python: Python programming for hackers and pentesters* (2nd ed.). No Starch Press.
- McKinney, W. (2022). *Python for data analysis* (3rd ed.). O'Reilly Media.
- Downey, A. (2015). *Think Python* (2nd ed.). O'Reilly Media.
- Stuttard, D., & Pinto, M. (2018). *The web application hacker's handbook* (2nd ed.). Wiley.
- Vieira, M., & Antunes, N. (2020). *Security testing for web applications*. Springer.

8 - Práctica Profesional II: Configuración y Administración de Redes

Instalación, configuración y administración básica de dispositivos de red (switches, routers y puntos de acceso), configuración de direccionamiento IP estático y dinámico, segmentación de redes mediante VLAN, configuración de subredes y routing básico, implementación de servicios de red (DNS, DHCP, servidor web y servidor de archivos), configuración y administración de redes inalámbricas seguras, implementación básica de firewalls y reglas de filtrado, configuración de redes privadas virtuales (VPN), monitoreo de tráfico y análisis mediante herramientas especializadas, detección de configuraciones inseguras y vulnerabilidades en redes locales, aplicación de principios de hardening en dispositivos de red, gestión de usuarios y control de accesos en infraestructura de red, implementación de copias de seguridad de configuraciones, simulación de incidentes de red y procedimientos básicos de respuesta, documentación técnica de topologías, configuraciones y medidas de seguridad implementadas.

Bibliografía sugerida

- Odom, W. (2020). *CCNA 200-301 official cert guide* (Vols. 1–2). Cisco Press.
- Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.
- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5th ed.). Pearson.
- Bejtlich, R. (2013). *The practice of network security monitoring*. No Starch Press.
- Scarfone, K., & Hoffman, P. (2016). *Guide to enterprise network security* (NIST Special Publication 800-41). National Institute of Standards and Technology.

9 - Legislación Informática y Protección de Datos

Marco jurídico de la informática y las tecnologías digitales, conceptos fundamentales de derecho informático, protección de datos personales y principios rectores (licitud, finalidad, proporcionalidad, seguridad y confidencialidad), derechos de los titulares de datos (acceso, rectificación, actualización y supresión), consentimiento informado y tratamiento legítimo de la información, responsabilidad de los responsables y encargados del tratamiento, medidas de seguridad jurídicas y técnicas para la protección de datos, normativa nacional e internacional en materia de protección de datos personales, delitos informáticos y tipificaciones penales asociadas (acceso indebido, fraude informático, daño informático, suplantación de identidad), evidencia digital y cadena de custodia básica, responsabilidad civil y penal en entornos digitales, regulación de comercio electrónico y firma digital, contratos informáticos, cumplimiento normativo (compliance) en seguridad de la información, estándares internacionales vinculados a la privacidad y protección de datos, análisis de casos jurisprudenciales relevantes, gobernanza digital y rol del profesional en ciberseguridad frente a obligaciones legales.

Bibliografía sugerida

- Greenleaf, G. (2018). *Asian data privacy laws: Trade and human rights perspectives* (2nd ed.). Oxford University Press.
- Kuner, C. (2020). *Transborder data flows and data privacy law*. Oxford University Press.
- Téllez Valdés, J. (2016). *Derecho informático*. McGraw-Hill Education.
- Solove, D. J., & Schwartz, P. M. (2020). *Information privacy law* (7th ed.). Wolters Kluwer.
- National Institute of Standards and Technology. (2020). *Privacy framework: A tool for improving privacy through enterprise risk management* (NIST SP 800-53 Rev. 5). NIST.

10 - Fundamentos de Ciberseguridad

Conceptos fundamentales de seguridad de la información, principios de confidencialidad, integridad y disponibilidad, autenticación, autorización y no repudio, amenazas, vulnerabilidades y riesgos en entornos digitales, actores y vectores de ataque, tipos de ataques informáticos (malware, phishing, ransomware, ataques de denegación de servicio, ingeniería social), modelos de seguridad y defensa en profundidad, gestión de identidades y control de accesos, fundamentos de criptografía aplicada (cifrado simétrico y asimétrico, funciones hash, certificados digitales), políticas de seguridad y normativas internacionales (ISO/IEC 27001, NIST), análisis y gestión de riesgos en sistemas informáticos, seguridad en redes y sistemas operativos, conceptos de hardening y segmentación, seguridad en aplicaciones web, introducción al hacking ético y pruebas de penetración, monitoreo de eventos de seguridad, respuesta básica ante incidentes, cultura organizacional de seguridad y concientización del usuario, gobernanza de la seguridad de la información y rol del técnico en ciberseguridad en entornos organizacionales.

Bibliografía sugerida

- Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.
- Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.
- Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). NIST.

- Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

11 -Criptografía y Seguridad de la Información

Fundamentos matemáticos de la criptografía, conceptos de confidencialidad, integridad y autenticidad, sistemas de cifrado simétrico y asimétrico, algoritmos clásicos y modernos de cifrado, funciones hash criptográficas, firmas digitales, infraestructura de clave pública (PKI), certificados digitales y autoridades certificadoras, protocolos criptográficos utilizados en redes (SSL/TLS, HTTPS, SSH), intercambio seguro de claves, criptografía aplicada a comunicaciones seguras, almacenamiento seguro de contraseñas y gestión de credenciales, autenticación multifactor, criptografía en sistemas distribuidos y entornos cloud, fundamentos de criptografía de clave pública basada en RSA y ECC, introducción a criptografía post-cuántica, análisis básico de vulnerabilidades criptográficas, ataques comunes (fuerza bruta, criptoanálisis, ataques de canal lateral), gestión segura de claves, estándares internacionales de seguridad de la información (ISO/IEC 27001, NIST), implementación práctica de mecanismos criptográficos en sistemas informáticos, rol de la criptografía en la protección de datos y en la ciberseguridad organizacional.

Bibliografía sugerida

- Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.
- Paar, C., & Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer.
- Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography* (3rd ed.). CRC Press.
- Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
- National Institute of Standards and Technology. (2023). *Digital signature standard (FIPS 186-5)*. NIST.

12 - Práctica Profesional III: Análisis de Vulnerabilidades

Metodología de análisis de vulnerabilidades en sistemas informáticos, identificación y clasificación de activos críticos, reconocimiento y recolección de información (footprinting y scanning), uso de herramientas de escaneo automatizado de vulnerabilidades, análisis manual de configuraciones inseguras en sistemas operativos, redes y aplicaciones, evaluación de puertos y servicios expuestos, identificación de vulnerabilidades comunes (OWASP Top 10, CVE), interpretación de reportes de seguridad y priorización según nivel de riesgo, fundamentos de pruebas de penetración controladas, explotación básica en entornos de laboratorio, análisis de configuraciones débiles en redes y servidores, revisión de políticas de autenticación y control de accesos, análisis de vulnerabilidades en aplicaciones web, pruebas de inyección y validación de entradas, documentación técnica de hallazgos, elaboración de informes ejecutivos y técnicos, recomendaciones de mitigación y remediación, buenas prácticas éticas y legales en pruebas de seguridad, simulación de escenarios de ataque controlado en entornos aislados, gestión del ciclo de mejora continua en seguridad.

Bibliografía sugerida

- Weidman, G. (2014). *Penetration testing: A hands-on introduction to hacking*. No Starch Press.
- Scarfone, K., Souppaya, M., & Cody, A. (2011). *Technical guide to information security testing and assessment (NIST SP 800-115)*. National Institute of Standards and Technology.
- Stuttard, D., & Pinto, M. (2018). *The web application hacker's handbook* (2nd ed.). Wiley.

- Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.
- OWASP Foundation. (2021). *OWASP top ten web application security risks*. https://owasp.org

13 - Gestión de Riesgos y Seguridad Organizacional

Conceptos fundamentales de gestión de riesgos en seguridad de la información, identificación y clasificación de activos organizacionales, análisis de amenazas y vulnerabilidades, evaluación y tratamiento de riesgos, metodologías de análisis de riesgo (cualitativas y cuantitativas), matrices de riesgo y priorización, ciclo de gestión de riesgos, políticas de seguridad de la información, marco normativo y estándares internacionales (ISO/IEC 27001, ISO/IEC 27005, NIST Risk Management Framework), continuidad del negocio y recuperación ante desastres (BCP y DRP), análisis de impacto en el negocio (BIA), gestión de incidentes de seguridad, establecimiento de controles preventivos, detectivos y correctivos, auditorías internas de seguridad, cultura organizacional de seguridad y concientización, gestión de terceros y proveedores críticos, gobernanza de la seguridad de la información, rol del responsable de seguridad (CISO) y estructura organizacional, documentación y reporte ejecutivo de riesgos, mejora continua del sistema de gestión de seguridad.

Bibliografía sugerida

- Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. NIST.
- International Organization for Standardization. (2018). *ISO/IEC 27005: Information security risk management*. ISO.
- Calder, A., & Watkins, S. (2015). *IT governance: An international guide to data security and ISO 27001/27002* (6th ed.). Kogan Page.
- Von Solms, R., & Van Niekerk, J. (2013). *From information security to cyber security*. Computers & Security, 38, 97–102.

14 - Seguridad en Sistemas y Aplicaciones

Principios de seguridad en sistemas operativos y aplicaciones, hardening de servidores Windows y Linux, gestión segura de configuraciones, control de accesos y privilegios mínimos, autenticación y autorización en sistemas empresariales, gestión de parches y actualizaciones, seguridad en aplicaciones web, vulnerabilidades comunes (OWASP Top 10), inyección SQL, cross-site scripting (XSS), cross-site request forgery (CSRF), validación y sanitización de entradas, seguridad en APIs y servicios web, mecanismos de autenticación segura (OAuth, JWT), protección contra ataques de fuerza bruta, gestión segura de sesiones, protección de bases de datos, registros y monitoreo de eventos de seguridad, implementación de firewalls de aplicaciones web (WAF), seguridad en entornos virtualizados y contenedores, análisis de código seguro (secure coding practices), pruebas de seguridad en el ciclo de desarrollo (DevSecOps), herramientas de análisis estático y dinámico de código, respuesta ante incidentes en aplicaciones, documentación técnica de medidas de protección implementadas.

Bibliografía sugerida

- Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.
- OWASP Foundation. (2021). *OWASP top ten web application security risks*. https://owasp.org

- Vieira, M., & Antunes, N. (2020). *Security testing for web applications*. Springer.
- Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
- McGraw, G. (2006). *Software security: Building security in*. Addison-Wesley.

15 - Ética y Responsabilidad Profesional en Entornos Digitales

Fundamentos éticos aplicados a las tecnologías digitales, principios de ética profesional en informática y ciberseguridad, responsabilidad social del profesional tecnológico, impacto social de la tecnología y la transformación digital, privacidad y protección de datos personales, confidencialidad y manejo responsable de la información, dilemas éticos en ciberseguridad, uso legítimo de herramientas de hacking ético, límites legales y profesionales en pruebas de seguridad, propiedad intelectual y derechos de autor en entornos digitales, ética en el desarrollo de software y prácticas de seguridad, transparencia y rendición de cuentas en sistemas automatizados, sesgos tecnológicos y responsabilidad en la toma de decisiones automatizadas, seguridad y derechos humanos en el entorno digital, ciberacoso y delitos informáticos desde una perspectiva ética, gobernanza digital y cumplimiento normativo, códigos de conducta profesional, integridad, confidencialidad y buenas prácticas en el ejercicio técnico, análisis de casos reales y toma de decisiones responsables en escenarios profesionales.

Bibliografía sugerida

- Johnson, D. G. (2021). *Computer ethics* (4th ed.). Pearson.
- Spinello, R. A. (2020). *Cyberethics: Morality and law in cyberspace* (7th ed.). Jones & Bartlett Learning.
- Floridi, L. (2013). *The ethics of information*. Oxford University Press.
- National Institute of Standards and Technology. (2020). *Privacy framework: A tool for improving privacy through enterprise risk management*. NIST.
- Association for Computing Machinery. (2018). *ACM code of ethics and professional conduct*. ACM.

16 - Inglés Técnico II

Profundización en comprensión lectora de textos técnicos avanzados en ciberseguridad y tecnología digital, análisis de documentación especializada sobre seguridad informática, redes, criptografía y gestión de incidentes, interpretación de normativas y estándares internacionales redactados en inglés (ISO, NIST, RFC), ampliación del vocabulario técnico específico en ciberseguridad, análisis de reportes de vulnerabilidades y documentos de fabricantes, comprensión de papers técnicos y artículos académicos del área, redacción de informes técnicos y ejecutivos en inglés, elaboración de documentación de incidentes y reportes de auditoría en idioma inglés, comunicación escrita formal en entornos profesionales tecnológicos, comprensión auditiva de presentaciones, webinars y conferencias técnicas internacionales, simulación de reuniones técnicas en inglés, análisis crítico de documentación de seguridad y manuales de configuración, uso autónomo de fuentes técnicas internacionales, desarrollo de habilidades para certificaciones técnicas que requieran comprensión de material en inglés.

Bibliografía sugerida

- Glendinning, E. H., & McEwan, J. (2013). *Oxford English for information technology* (2nd ed.). Oxford University Press.
- Hewings, M. (2013). *Advanced grammar in use* (3rd ed.). Cambridge University Press.

- Murphy, R. (2019). *English grammar in use* (5th ed.). Cambridge University Press.
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. NIST.
- Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.

17 - Práctica Profesional IV: Gestión de Incidentes y Monitoreo

Fundamentos de gestión de incidentes de seguridad informática, ciclo de vida del incidente (detección, análisis, contención, erradicación y recuperación), identificación y clasificación de eventos de seguridad, monitoreo continuo de infraestructura tecnológica, uso de herramientas de SIEM (Security Information and Event Management), análisis de logs y correlación de eventos, detección de anomalías en redes y sistemas, indicadores de compromiso (IoC) y amenazas persistentes avanzadas (APT), respuesta ante incidentes en entornos corporativos, preservación de evidencia digital y cadena de custodia básica, coordinación de equipos de respuesta (CSIRT/SOC), elaboración de planes de respuesta ante incidentes, gestión de crisis y comunicación interna, simulación de escenarios de ataque (tabletop exercises), análisis forense digital introductorio, mitigación de impactos y restauración de servicios, documentación técnica y elaboración de reportes ejecutivos, mejora continua de procesos de monitoreo y respuesta, cumplimiento normativo en la gestión de incidentes, buenas prácticas internacionales (NIST, ISO 27035), ética profesional en la gestión de eventos de seguridad.

Bibliografía sugerida

- Casey, E. (2011). *Digital evidence and computer crime* (3rd ed.). Academic Press.
- Scarfone, K., Kent, K., & Souppaya, M. (2012). *Computer security incident handling guide (NIST SP 800-61 Rev. 2)*. National Institute of Standards and Technology.
- Bejtlich, R. (2013). *The practice of network security monitoring*. No Starch Press.
- Nelson, B., Phillips, A., & Steuart, C. (2018). *Guide to computer forensics and investigations* (6th ed.). Cengage Learning.
- International Organization for Standardization. (2016). *ISO/IEC 27035: Information security incident management*. ISO.

18 - Seguridad en Entornos Cloud e Infraestructuras Críticas

Fundamentos de seguridad en computación en la nube, modelos de servicio (IaaS, PaaS, SaaS) y modelo de responsabilidad compartida, arquitectura de seguridad en entornos cloud públicos, privados e híbridos, gestión de identidades y accesos en la nube (IAM), configuración segura de servicios y recursos virtuales, segmentación de redes virtuales, cifrado de datos en tránsito y en reposo en entornos cloud, gestión de claves y certificados, seguridad en contenedores y entornos virtualizados, monitoreo y registro de eventos en plataformas cloud, detección de configuraciones inseguras, cumplimiento normativo en entornos de nube, evaluación de riesgos en infraestructuras críticas, protección de sistemas industriales y entornos OT/ICS, amenazas específicas a infraestructuras críticas, continuidad operativa y resiliencia en sistemas estratégicos, implementación de controles de seguridad en servicios esenciales, análisis de incidentes en entornos distribuidos, estándares y marcos internacionales para protección de infraestructuras críticas (NIST, ISO 27019), gobernanza y gestión de riesgos en servicios cloud, buenas prácticas de seguridad en arquitecturas modernas.

Bibliografía sugerida

- Stallings, W. (2018). *Cloud computing: Concepts, technology & architecture*. Pearson.

- Rittinghouse, J. W., & Ransome, J. F. (2017). *Cloud computing: Implementation, management, and security* (2nd ed.). CRC Press.
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). NIST.
- Grance, T., & Mell, P. (2011). *The NIST definition of cloud computing (SP 800-145)*. National Institute of Standards and Technology.
- International Organization for Standardization. (2017). *ISO/IEC 27017: Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. ISO.

19 - Auditoría y Normativas de Seguridad Informática

Fundamentos de auditoría en sistemas de información, objetivos y alcance de auditorías de seguridad informática, tipos de auditoría (interna, externa, técnica y de cumplimiento), planificación y ejecución de auditorías, identificación de controles y evaluación de su eficacia, análisis de brechas de seguridad (gap analysis), marcos normativos y estándares internacionales de seguridad de la información (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, NIST Cybersecurity Framework, COBIT), gobierno y gestión de la seguridad de la información, políticas y procedimientos organizacionales, evaluación de controles técnicos y administrativos, revisión de configuraciones de seguridad en sistemas y redes, auditoría de accesos y gestión de identidades, análisis de cumplimiento legal y regulatorio, elaboración de informes técnicos y ejecutivos de auditoría, recomendaciones de mejora y planes de acción correctiva, seguimiento de hallazgos y mejora continua, ética profesional en procesos de auditoría, confidencialidad y manejo de evidencia documental, rol del auditor en entornos digitales y organizacionales.

Bibliografía sugerida

- Calder, A., & Watkins, S. (2015). *IT governance: An international guide to data security and ISO 27001/27002* (6th ed.). Kogan Page.
- ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. NIST.
- International Organization for Standardization. (2022). *ISO/IEC 27001: Information security management systems – Requirements*. ISO.
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

20 - Liderazgo, Comunicación y Trabajo en Equipos Tecnológicos

Fundamentos de liderazgo en entornos tecnológicos, estilos de liderazgo y su aplicación en equipos de tecnología, habilidades interpersonales y comunicación efectiva, comunicación oral y escrita en contextos técnicos, gestión de conflictos en equipos de trabajo, toma de decisiones colaborativa, trabajo en equipos interdisciplinarios, dinámica y roles en equipos tecnológicos, motivación y gestión del desempeño, liderazgo ético y responsabilidad profesional, metodologías ágiles y trabajo colaborativo (Scrum, Kanban), planificación y coordinación de tareas en proyectos tecnológicos, gestión del cambio organizacional en procesos de transformación digital, inteligencia emocional aplicada al entorno profesional, negociación y comunicación con áreas no técnicas, cultura organizacional en empresas tecnológicas, presentación de informes técnicos y ejecutivos, gestión del tiempo y organización del trabajo, mejora continua y aprendizaje profesional permanente.

Bibliografía sugerida

- Robbins, S. P., & Judge, T. A. (2022). *Organizational behavior* (19th ed.). Pearson.
- Goleman, D. (2013). *Primal leadership: Unleashing the power of emotional intelligence*. Harvard Business Review Press.
- Sutherland, J. (2014). *Scrum: The art of doing twice the work in half the time*. Crown Business.
- Lencioni, P. (2002). *The five dysfunctions of a team*. Jossey-Bass.
- Project Management Institute. (2021). *A guide to the project management body of knowledge (PMBOK® Guide)* (7th ed.). PMI.

21 - Práctica Profesional V – Proyecto Final Integrador

Formulación integral de un proyecto aplicado a ciberseguridad y protección de sistemas digitales, identificación de una problemática real en entornos organizacionales, análisis de contexto tecnológico y evaluación de riesgos, definición de objetivos técnicos y alcance del proyecto, diseño de arquitectura de seguridad acorde a estándares internacionales, implementación de soluciones técnicas (hardening, segmentación de red, políticas de acceso, monitoreo, cifrado, respuesta ante incidentes), aplicación de metodologías de análisis de vulnerabilidades y gestión de riesgos, integración de herramientas de monitoreo y gestión de incidentes, documentación técnica del proceso de implementación, evaluación de cumplimiento normativo y buenas prácticas (ISO 27001, NIST, marcos regulatorios vigentes), análisis de impacto organizacional y propuesta de mejora continua, elaboración de informe técnico y ejecutivo, defensa oral del proyecto ante tribunal académico, reflexión ética y profesional sobre la intervención realizada, integración de competencias técnicas, normativas y organizacionales desarrolladas durante la carrera.

Bibliografía sugerida

- Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. NIST.
- International Organization for Standardization. (2022). *ISO/IEC 27001: Information security management systems – Requirements*. ISO.
- Scarfone, K., Kent, K., & Souppaya, M. (2012). *Computer security incident handling guide (NIST SP 800-61 Rev. 2)*. National Institute of Standards and Technology.

10.- METODOLOGÍA DE ENSEÑANZA Y EVALUACIÓN

10.1.- Enfoque metodológico

La propuesta pedagógica de la Tecnicatura Universitaria en Ciberseguridad y Protección de Sistemas Digitales se fundamenta en un enfoque de formación tecnológica, aplicada y orientada a la protección de infraestructuras digitales, centrada en el desarrollo de competencias profesionales acordes al perfil del egresado y a las demandas del ecosistema tecnológico y de la economía digital.

El proceso de enseñanza y aprendizaje se concibe como un trayecto formativo progresivo que articula fundamentos informáticos, redes y sistemas con la aplicación práctica de herramientas

y metodologías de ciberseguridad. Se prioriza la integración sistemática entre teoría y práctica, vinculando los contenidos académicos con escenarios de aplicación propios de la gestión de vulnerabilidades, la protección de redes, la respuesta a incidentes y la implementación de políticas de seguridad de la información.

La carrera adopta un enfoque de formación por competencias, entendidas como la integración de saberes conceptuales, operativos y actitudinales que permiten al estudiante desempeñarse adecuadamente en contextos reales o simulados de seguridad informática, bajo estándares de calidad, normativas vigentes, buenas prácticas técnicas y ética profesional.

Estrategias de enseñanza

Las estrategias de enseñanza se orientan a favorecer la apropiación de los fundamentos técnicos y el desarrollo de habilidades operativas mediante modalidades didácticas acordes a una tecnicatura universitaria de carácter práctico y tecnológico.

Entre las principales estrategias se contemplan:

- Clases teórico-prácticas destinadas a la introducción y aplicación de conceptos de redes, sistemas operativos, arquitectura informática y seguridad de la información.
- Laboratorios de configuración y administración de sistemas y redes en entornos controlados.
- Simulación de escenarios de ciberataques y análisis de incidentes en laboratorios virtuales.
- Resolución de casos reales o simulados vinculados a vulnerabilidades, gestión de riesgos y protección de infraestructuras digitales.
- Desarrollo de proyectos progresivos orientados al diseño e implementación de políticas y soluciones de seguridad informática.
- Talleres de integración tecnológica en los espacios de Práctica Profesionalizante, con énfasis en monitoreo, análisis de eventos, configuración segura y respuesta ante incidentes.
- Actividades de trabajo colaborativo bajo dinámicas similares a entornos reales de equipos de seguridad (SOC, soporte técnico, administración de redes).
- Estas estrategias promueven la participación activa del estudiante, favorecen el aprendizaje basado en problemas y proyectos, y facilitan la transferencia directa de conocimientos al ámbito profesional.

Articulación entre teoría y práctica

La propuesta pedagógica prevé una articulación permanente entre teoría y práctica a lo largo de toda la carrera. Los contenidos teóricos constituyen el soporte conceptual indispensable para comprender los principios de seguridad informática, mientras que las instancias prácticas permiten su aplicación en la configuración, monitoreo y protección de sistemas digitales.

Las Prácticas Profesionalizantes I, II y III constituyen el eje integrador del trayecto formativo, posibilitando la aplicación progresiva de competencias vinculadas a la administración segura de sistemas, análisis de vulnerabilidades, implementación de controles y gestión de incidentes. La Práctica Final Integradora consolida estos saberes mediante el desarrollo de un proyecto aplicado de protección de infraestructura digital en un contexto real o simulado.

Modalidad de cursado y uso de entornos virtuales

La carrera se desarrolla bajo una modalidad que combina instancias presenciales y virtuales de manera planificada. Las actividades presenciales se destinan prioritariamente a laboratorios técnicos, simulaciones de incidentes, evaluaciones prácticas y desarrollo colaborativo de proyectos de seguridad. Las instancias virtuales se orientan al abordaje de contenidos teóricos, prácticas guiadas, análisis de casos y uso de plataformas de laboratorio remoto.

El uso de entornos virtuales, laboratorios de simulación, máquinas virtuales, plataformas cloud y herramientas colaborativas forma parte integral del proceso formativo, dado que constituyen el entorno real de desempeño profesional en el campo de la ciberseguridad.

Rol docente y del estudiante

El docente asume funciones de planificación, orientación técnica, acompañamiento y supervisión del proceso formativo, actuando como facilitador en la resolución de problemas de seguridad y garante de la calidad académica y técnica.

El estudiante es considerado un sujeto activo, responsable de su aprendizaje, del trabajo colaborativo y del desarrollo progresivo de competencias técnicas, analíticas y éticas acordes al perfil profesional en ciberseguridad.

Articulación con el sistema de evaluación

La propuesta pedagógica se articula coherentemente con el sistema de evaluación por competencias adoptado por la carrera, asegurando correspondencia entre objetivos formativos, estrategias de enseñanza y criterios de evaluación. La evaluación se integra al proceso formativo como instancia de retroalimentación y mejora continua.

10.2.- Evaluación

De acuerdo con el modelo formativo institucional, la evaluación en la Tecnicatura Universitaria en Ciberseguridad y Protección de Sistemas Digitales se estructura a partir de normas de competencia que definen objetivos de aprendizaje, criterios de desempeño y evidencias verificables.

La evaluación se concibe como un proceso continuo, formativo y estratégico, orientado a determinar los niveles de competencia alcanzados en la identificación, prevención y mitigación de riesgos y amenazas digitales.

Ejes de la evaluación integral

La evaluación se organiza en cuatro ejes:

a. Fundamentos técnicos y metodológicos (Saber): Se evalúa la comprensión y aplicación de principios de redes, sistemas operativos, arquitectura informática, criptografía básica y fundamentos de seguridad de la información.

b. Dominio operativo y tecnológico (Saber hacer): Se observa la capacidad para configurar sistemas seguros, identificar vulnerabilidades, aplicar herramientas de análisis, monitorear eventos y participar en la gestión de incidentes.

c. Gestión de seguridad y cumplimiento normativo (Saber hacer con estándares): Se verifica la aplicación de buenas prácticas, políticas de seguridad, documentación técnica, gestión de riesgos y cumplimiento de normativas de protección de datos.

d. Desempeño profesional, ético y transversal (Saber ser): Se evalúa la responsabilidad en el manejo de información sensible, la confidencialidad, el trabajo en equipo, la comunicación técnica y la conducta ética profesional.

Evidencias de competencia

Las evidencias se organizan en:

- **Evidencias de conocimiento:** evaluaciones teóricas, análisis conceptual y resolución de problemas técnicos.
- **Evidencias de desempeño:** configuración práctica de sistemas, simulaciones de incidentes, análisis de vulnerabilidades y aplicación de controles de seguridad.

- **Evidencias de producto:** proyectos integradores, informes técnicos de auditoría o incidentes, configuraciones documentadas y propuestas de mejora en seguridad digital.

La evaluación como proceso de mejora continua

La evaluación no se limita a la acreditación, sino que constituye un dispositivo de seguimiento del desarrollo de competencias técnicas y profesionales. Permite validar la pertinencia de los contenidos y la adecuación de las Prácticas Profesionalizantes a las dinámicas cambiantes del campo de la ciberseguridad, asegurando la actualización permanente del trayecto formativo frente a la evolución de amenazas y tecnologías.