



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

CÓRDOBA, 26 de noviembre de 2025.-

VISTO:

La propuesta de formación académica de pregrado que busca formar profesionales capacitados en la protección de la información y la infraestructura crítica;

Y CONSIDERANDO:

Que la creciente dependencia de tecnologías digitales en todos los ámbitos de la vida cotidiana, desde la interacción personal hasta las operaciones empresariales y gubernamentales, ha llevado a un aumento en la exposición a amenazas cibernéticas.

Que, en tal sentido, resulta oportuno brindar una oferta académica orientada a la formación de profesionales capaces de prevenir, detectar y mitigar incidentes de ciberataques, protegiendo tanto la información personal como la seguridad nacional.

Que el Instituto de Gestión e Innovación Tecnológica y Productiva de la Universidad Provincial de Córdoba tiene como misión generar conocimientos, formar profesionales altamente capacitados, promover la actualización disciplinar continua, fomentar la investigación, impulsar la extensión universitaria y brindar asesoría técnica y cooperación a la comunidad y el sector productivo.

Que dicha institución se propone colaborar a través de la generación de ofertas formativas relacionadas con capacidades de uso y desarrollo de tecnología aplicada a diferentes procesos productivos en la provincia de Córdoba.



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

Que la formación de un/a Técnico/a en Ciberseguridad en el ámbito de la Universidad Provincial de Córdoba busca dar una respuesta a las tendencias y necesidades actuales del mercado laboral, a la demanda de innovación tecnológica y a la necesidad de contar con profesionales formados en áreas estratégicas de desarrollo de software que contribuirán al crecimiento y la competitividad de la industria tecnológica a nivel local y nacional, fortaleciendo la economía del conocimiento y posicionando a la región como un centro de talento calificado en tecnología.

Que, conforme se fundamenta en su diseño curricular, la ciberseguridad se erige como un campo interdisciplinario que integra conocimiento de la informática, telecomunicaciones, derecho, ética y administración.

Que la presente propuesta formativa se enfoca en brindar una sólida formación técnica y teórica que comprenda no solo las herramientas y tecnologías de seguridad, sino también los principios fundamentales de gestión del riesgo, leyes y normativas vigentes, y las mejores prácticas internacionales en la materia.

Que se espera que el/la Técnico/a Universitario/a en Ciberseguridad cuente con una sólida base en fundamentos y habilidades en ciberseguridad, con capacidad de participar en el diseño, la implementación y el sostenimiento de soluciones innovadoras y medidas de seguridad para proteger activos digitales, tanto en entornos públicos como privados, en entornos productivos, industriales y de servicios.

Que la oferta cuenta con el visto bueno de la Secretaría Académica y de Posgrado de la Universidad Provincial de Córdoba.

Que, en razón de todo ello, resulta oportuno crear la carrera de pregrado: "Tecnicatura Universitaria en Ciberseguridad" que otorga el título de "Técnico/a Universitario/a en Ciberseguridad".



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

Que conforme a lo dispuesto por el art. 14 de la Ley Provincial Nro. 9.375, su modificatoria Ley Provincial Nro. 10.206, el Decreto Provincial Nro. 1.080/18, la Ley Provincial Nro. 10.704, el Decreto Provincial Nro. 744/22, la Resolución del Ministerio de Educación Nro. 591 - Letra D/2024, la Ley Provincial Nro. 10.953 y demás normativa aplicable, corresponden a la Rectora Normalizadora las atribuciones propias de su cargo y a su vez aquellas que el Estatuto les asigna a los futuros órganos de gobierno de la Universidad.

En virtud de ello, la normativa citada y en uso de sus atribuciones;

**LA RECTORA NORMALIZADORA
DE LA UNIVERSIDAD PROVINCIAL DE CÓRDOBA
RESUELVE:**

Artículo 1º: CRÉASE, bajo el ámbito del Instituto de Gestión e Innovación Tecnológica y Productiva dependiente de la Universidad Provincial de Córdoba, la carrera de pregrado “*Tecnicatura Universitaria en Ciberseguridad*”, con una duración de tres (3) años y una carga horaria de un mil trescientos setenta y seis (1376) horas reloj, la cual otorga el título de “*Técnico/a Universitario/a en Ciberseguridad*”.

Artículo 2º: APRUÉBASE, el plan de estudio que en Anexo se acompaña y forma parte de la presente resolución.

Artículo 3º: PROTOCOLÍCESE, comuníquese y archívese.

RESOLUCIÓN Nro. 477.-

477



Esp. María Julia Oliva Cúneo
Rectora Normalizadora
Universidad Provincial de Córdoba



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

ANEXO

UNIVERSIDAD PROVINCIAL DE CÓRDOBA INSTITUTO DE GESTIÓN E INNOVACIÓN TECNOLÓGICA Y PRODUCTIVA TECNICATURA UNIVERSITARIA EN CIBERSEGURIDAD

A 1. Identificación de la carrera

1.1. Nombre de la carrera:

Tecnicatura Universitaria en Ciberseguridad

1.2. Nombre del título a otorgar

Técnico/a Universitario/a en Ciberseguridad

1.3. Duración estimada

Tres (3) años

1.4. Carga horaria total

1376 (un mil trescientos setenta y seis) horas reloj

1.5. Nivel académico universitario

Pregrado

1.6. Modalidad

Presencial

1.7. Ubicación en la estructura institucional

Instituto de Gestión e Innovación Tecnológica y Productiva

1.8. Fundamentación

La creciente dependencia de tecnologías digitales en todos los ámbitos de la vida cotidiana, desde la interacción personal hasta las operaciones empresariales y gubernamentales, ha llevado a un aumento exponencial en la exposición a amenazas cibernéticas. En este contexto, la creación de una Tecnicatura Universitaria en Ciberseguridad se justifica tanto por la evolución del campo disciplinar como por la necesidad urgente de formar profesionales capacitados en la protección de la información y la infraestructura crítica.



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

La ciberseguridad se erige como un campo interdisciplinario que integra conocimiento de la informática, telecomunicaciones, derecho, ética y administración. Esta Tecnicatura se enfoca en brindar una sólida formación técnica y teórica que comprenda no solo las herramientas y tecnologías de seguridad, sino también los principios fundamentales de gestión del riesgo, leyes y normativas vigentes, y las mejores prácticas internacionales en la materia. Los egresados estarán equipados para abordar los desafíos emergentes en un entorno en constante evolución considerando las dimensiones éticas y sociales.

Esta Tecnicatura responde a la necesidad social de contar con profesionales que sean capaces de prevenir, detectar y mitigar incidentes de ciberataques, protegiendo tanto la información personal como la seguridad nacional. Además, se abordarán temas de concienciación y educación sobre ciberseguridad, contribuyendo así a una cultura de responsabilidad digital en la sociedad.

Con la incorporación de esta Tecnicatura Universitaria, la Universidad Provincial de Córdoba, busca dar una respuesta a las tendencias y necesidades actuales del mercado laboral, a la demanda de innovación tecnológica y a la necesidad de contar con profesionales formados en áreas estratégicas de desarrollo de software que contribuirán al crecimiento y competitividad de la industria tecnológica a nivel local y nacional, fortaleciendo la economía del conocimiento y posicionando a la región como un centro de talento calificado en tecnología.

2. Horizontes de la carrera

2.1. Objetivos de la carrera

Objetivo general

Formar técnicos universitarios con una sólida base en fundamentos y habilidades en ciberseguridad, capaces de participar en el diseño, implementar y mantener soluciones innovadoras y medidas de seguridad para proteger activos digitales, tanto en entornos públicos como privados, en entornos productivos, industriales y de servicios.

Objetivos específicos

- Proveer fundamentos sólidos en sistemas informáticos, redes, programación y bases de datos.
- Capacitar en la evaluación de riesgos, análisis de vulnerabilidades y pruebas de penetración.



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

- Formar en criptografía, firma digital, infraestructura PKI y controles tácticos de seguridad.
- Otorgar conocimientos sobre las normas y marcos legales vigentes tanto a nivel nacional como internacional en ciberseguridad y delitos informáticos.
- Brindar herramientas para afrontar amenazas emergentes.
- Fomentar un enfoque ético y legal en la implementación de soluciones de Seguridad de la información, seguridad informática y ciberseguridad.
- Formar en competencias de gestión y comunicación para el trabajo colaborativo y de servicio.

2.2. Perfil del egresado

Se espera que el/la graduado/a de la Tecnicatura Universitaria en Ciberseguridad haya adquirido conocimientos, habilidades y/o actitudes para:

- La implementación de medidas de seguridad en sistemas, redes, servidores, bases de datos y aplicaciones.
- La participación en auditorías técnicas, pruebas de penetración y análisis de vulnerabilidades.
- La gestión de incidentes de ciberseguridad y la participación en equipos de respuesta.
- La asistencia en la adopción de normas y marcos regulatorios internacionales.
- El conocimiento y la aplicación de la legislación argentina en delitos informáticos.
- La intervención en proyectos de seguridad en entornos industriales, comercio electrónico y fuerzas de seguridad.
- La colaboración con organismos de seguridad en la prevención, detección y respuesta ante amenazas cibernéticas.
- La participación en equipos multidisciplinarios con capacidad de comunicación efectiva y toma de decisiones técnicas y éticas.



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

- La integración de conocimientos éticos y de sostenibilidad en la toma de decisiones técnicas, junto con habilidades y competencias de gestión y comunicación.

2.3. Alcances del título

“La responsabilidad primaria y la toma de decisiones la ejerce en forma individual y exclusiva el poseedor del título con competencia reservada según el régimen del artículo 43 LES”. Por tal motivo, el/la Técnico/a Universitario/a en Ciberseguridad por sí, le está vedado realizar dichas actividades.

Los/as egresados/as de la Tecnicatura Universitaria en Ciberseguridad estarán habilitados/as para:

- Participar en el análisis, diseño e implementación de políticas de seguridad de la información, y medidas técnicas de seguridad.
- Aplicar herramientas de seguridad a nivel de redes, servidores, sistemas operativos y bases de datos, y en el desarrollo de aplicaciones.
- Participar en el análisis de riesgos y asesoramiento sobre controles y medidas de mitigación.
- Integrar equipos de respuesta ante incidentes en entornos públicos y privados.
- Asistir en tareas de investigación digital a diversos organismos públicos y Fuerzas de Seguridad.
- Participar en auditorías, análisis de vulnerabilidades y continuidad operativa.
- Colaborar en el desarrollo de programas de capacitación en ciberseguridad.

3. Diseño curricular de la carrera

3.1. Requisitos de ingreso

Las condiciones de ingreso a la carrera son las estipuladas en el artículo 7 de la LES N° 24.521: “Para ingresar como alumno a las instituciones de nivel superior, se debe haber aprobado el nivel medio o el ciclo polimodal de enseñanza. Excepcionalmente, los mayores de 25 años que no reúnan esa condición, podrán ingresar siempre que demuestren, a través de las evaluaciones que las provincias, la Municipalidad de la Ciudad de Buenos Aires o las universidades en su caso establezcan, que tienen



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

preparación y/o experiencia laboral acorde con los estudios que se proponen iniciar, así como aptitudes y conocimientos suficientes para cursarlos satisfactoriamente”.

3.2. Requisitos de egreso

Para obtener el título de Técnico/a Universitario/a en Ciberseguridad, los/as estudiantes deberán:

- Aprobar el total de unidades curriculares contempladas en el plan de estudios.
- Aprobar examen de suficiencia de idioma inglés.



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

3.3. Estructura Curricular

a. Unidades Curriculares, código, formato, asignación horaria semanal, total y condición académica

1° Año											
Unidades curriculares semestrales											
1° semestre						2° semestre					
Unidad curricular	Cód. UC	Formato	Horas reloj anuales	Horas reloj semanales	Condición académica	Unidad curricular	Cód. UC	Formato	Horas reloj anuales	Horas reloj semanales	Condición académica
Matemática 1	01	Asignatura	48	3	Promoción Regular Libre	Matemática 2	06	Asignatura	64	4	Promoción Regular Libre
Computación y Sistemas Operativos	02	Asignatura	64	4	Promoción Regular Libre	Programación	07	Asignatura	64	4	Promoción Regular Libre
Introducción a la Ciberseguridad	03	Asignatura	48	3	Promoción Regular Libre	Redes de Computadoras	08	Asignatura	64	4	Promoción Regular Libre
Comunicación Profesional	04	Asignatura	32	2	Promoción Regular Libre	Práctica Profesionalizante e 1	09	Práctica Profesionalizante	32	2	Promoción Regular Libre
Normas y Estándares de Seguridad	05	Asignatura	48	3	Promoción Regular Libre						

Totales 1° año

Unidades curriculares: Nueve (9). Cinco (5) en primer semestre y cuatro (4) en segundo semestre.

Horas reloj anuales: Cuatrocientas sesenta y cuatro (464)

Horas reloj semanales: Quince (15) en primer semestre y catorce (14) en segundo semestre.



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

2° Año

Unidades curriculares semestrales

1° semestre						2° semestre					
Unidad curricular	Cód. UC	Formato	Horas reloj anuales	Horas reloj semanales	Condición académica	Unidad curricular	Cód. UC	Formato	Horas reloj anuales	Horas reloj semanales	Condición académica
Bases de Datos y Seguridad	10	Asignatura	48	3	Promoción Regular Libre	Seguridad en el Desarrollo de Aplicaciones	15	Asignatura	48	3	Promoción Regular Libre
Seguridad en Redes de Computadoras	11	Asignatura	48	3	Promoción Regular Libre	Análisis de Riesgos y Gestión de Incidentes	16	Asignatura	48	3	Promoción Regular
Seguridad de Sistemas Operativos	12	Asignatura	48	3	Promoción Regular Libre	Auditoría y Pentesting	17	Asignatura	48	3	Promoción Regular Libre
Legislación en Ciberseguridad	13	Asignatura	32	2	Promoción Regular Libre	Ciberdelitos Informáticos	18	Asignatura	48	3	Promoción Regular Libre
Gestión de Proyectos	14	Asignatura	32	2	Promoción Regular	Clave Pública y Firma Digital	19	Asignatura	32	2	Promoción Regular
						Práctica Profesionalizante 2	20	Práctica Profesionalizante	32	2	Promoción Regular

Totales 2° año

Unidades curriculares: Once (11). Cinco (5) en primer semestre y seis (6) en segundo semestre.

Horas reloj anuales: Cuatrocientas sesenta y cuatro (464)

Horas reloj semanales: Trece (13) en primer semestre y dieciséis (16) en segundo semestre.



Mgter. Jorge Omar Abal Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

3° Año											
Unidades curriculares semestrales											
1° semestre						2° semestre					
Unidad curricular	Có d. UC	Formato	Horas reloj anuales	Horas reloj semanales	Condición académica	Unidad curricular	Có d. UC	Formato	Horas reloj anuales	Horas reloj semanales	Condición académica
Amenazas Emergentes y Ciberseguridad	21	Asignatura	48	3	Promoción Regular Libre	Seguridad en Comercio Electrónico	26	Asignatura	64	4	Promoción Regular Libre
Seguridad en la Nube	22	Asignatura	48	3	Promoción Regular Libre	Ciberdefensa. Ciberinteligencia y Guerra Cibernética	27	Asignatura	48	3	Promoción Regular Libre
Ciberseguridad Industrial y Sistemas Críticos	23	Asignatura	64	4	Promoción Regular Libre	Ciberseguridad para Fuerzas de Seguridad y Organismos Públicos	28	Asignatura	64	4	Promoción Regular
Ética y Deontología Profesional	24	Asignatura	32	2	Promoción Regular Libre	Práctica Profesionalizante 4	29	Práctica Profesionalizante	48	3	Promoción Regular
Práctica Profesionalizante 3	25	Práctica Profesionalizante	32	2	Promoción Regular						

Totales 3° año

Unidades curriculares: Nueve (9). Cinco (5) en primer semestre y cuatro (4) en segundo semestre.

Horas reloj anuales: Cuatrocientas cuarenta y ocho (448)

Horas reloj semanales: Catorce (14) en primer semestre y catorce (14) en segundo semestre.

Horas Totales de la carrera: 1376 horas reloj



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

B.- Modalidad de dictado de las unidades curriculares

Todas las unidades curriculares son de modalidad presencial.

C.- Contenidos mínimos de las unidades curriculares

PRIMER AÑO

01 - Matemática 1

Conjuntos, relaciones y funciones. Álgebra lineal: matrices y determinantes. Sistemas de ecuaciones lineales. Introducción a matemática discreta: lógica proposicional, tablas de verdad, álgebra de proposiciones, combinatoria, teoría de grafos y árboles.

02 - Computación y Sistemas Operativos

Componentes de una computadora. Representación de datos. Arquitectura básica. Tipos de sistemas operativos. Procesos, memoria, archivos y dispositivos. Interfaces CLI y GUI. Introducción a Windows y Linux.

03 - Introducción a la Ciberseguridad

Conceptos de seguridad de la información, seguridad informática y ciberseguridad. Confidencialidad, integridad y disponibilidad (CIA). El cubo de la seguridad. Brechas, vulnerabilidades y riesgos. Ciberseguridad en organizaciones públicas y privadas. Tipos de amenazas y actores.

04 - Comunicación Profesional

Técnicas de redacción y presentación profesional. Documentación técnica. Ética en tecnología y privacidad. Comunicación efectiva, trabajo en equipo, liderazgo y responsabilidad profesional.

05 - Normas y Estándares de Seguridad

Introducción a la familia ISO/IEC 27000. Análisis de ISO/IEC 27001 y 27002. Sistema de Gestión de Seguridad de la Información. Ciclo PDCA. Gestión de riesgos. Controles de seguridad. Introducción a NIST Cybersecurity Framework. Políticas y procedimientos de seguridad de la información.



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

06 - Matemática 2

Cálculo en una variable: Funciones. Límite. Continuidad. Cálculo diferencial e integral. Análisis de variación de funciones. Aplicaciones. Introducción a la criptografía: Historia. Cifrado simétrico y asimétrico. Hashing. Aplicaciones en protección de datos.

07 - Programación

Algoritmos, estructuras de control, funciones. Estructuras de datos (listas, diccionarios, pilas, colas, árboles). Programación orientada a objetos: clases, objetos, encapsulamiento, herencia, polimorfismo. Testeo y buenas prácticas. Python u otro lenguaje de alto nivel.

08 - Redes de Computadoras

Modelo OSI y TCP/IP. Topologías, medios y dispositivos de red. Direccionamiento IPv4/IPv6. Subredes. Protocolos básicos (ARP, ICMP, DNS, DHCP). Introducción a la configuración y gestión de redes.

09 - Práctica Profesionalizante 1

El campo laboral del Técnico en Ciberseguridad. Tareas y acciones en el rol de Técnico en Ciberseguridad. Observación y entrevistas en diversos entornos, públicos y privados, industriales, productivos, y de servicios. Análisis de caso tomando como referencia normas y estándares de seguridad.

SEGUNDO AÑO

10 - Bases de Datos y Seguridad

Modelo relacional y NoSQL. Diseño lógico y físico. SQL. DER. Normalización. Seguridad en BD: control de accesos, cifrado, auditoría, SQLi y hardening de motores de bases de datos.

11 - Seguridad en Redes de Computadoras

Seguridad perimetral. Firewalls, NAT, VPN. IDS/IPS. Segmentación de redes. Protocolos seguros. Hardening de routers y switches. Vulnerabilidades comunes. Seguridad en profundidad.



Mgter. Jorge Omar Abel Jalmeiz
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

12 – Seguridad de Sistemas Operativos

Configuración segura. Gestión de usuarios, servicios y permisos. Auditoría y logs. Automatización con scripts. Linux hardening y seguridad en Windows. Herramientas de análisis.

13 - Legislación en Ciberseguridad

Normativa argentina sobre delitos informáticos. Leyes 25.326, 26.388 y otras. Derechos digitales. Convenios internacionales. Responsabilidad penal y civil. Evidencia digital. Seguridad jurídica.

14 - Gestión de Proyectos

Fundamentos de gestión de proyectos tecnológicos. Ciclo de vida de proyectos. Uso de metodologías ágiles y tradicionales Scrum, Kanban, Lean. Documentación, gestión de equipos y presentación a stakeholders. Planificación en ciberseguridad.

15 - Seguridad en el Desarrollo de Aplicaciones

OWASP Top 10. Ataques (XSS, SQLi, CSRF, SSRF, IDOR). Escaneo de vulnerabilidades. Prácticas de desarrollo seguro. Seguridad en el desarrollo de aplicaciones Web y Móviles. Herramientas: Burp Suite, ZAP.

16 - Análisis de Riesgos y Gestión de Incidentes

Metodologías de análisis de riesgo (OCTAVE, MAGERIT, otras). Evaluación de impacto y probabilidad. Planes de continuidad y recuperación. Gestión de incidentes. Coordinación con CERT/CSIRT. Indicadores y reportes.

17 - Auditoría y Pentesting

Proceso de auditoría técnica. Recolección de información, escaneo, explotación. OSSTMM y OWASP. Herramientas: Metasploit, Nmap. Simulación de ataques (red y aplicación). Red team y blue team.

18 - Ciberdelitos y Delitos Informáticos

Tipologías delictivas: phishing, ransomware, grooming, fraudes. Ingeniería social. Crimen organizado digital. Evidencia digital. Marco penal argentino. Cooperación internacional. Delitos contra menores y personas.



Mgtr. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

19 - Clave Pública y Firma Digital

Fundamentos de PKI. Certificados digitales, CA y revocación. Firma digital. Infraestructura nacional y usos en servicios digitales. Aspectos legales prácticos.

20 - Práctica Profesionalizante 2

Auditoría en Sistemas Operativos y en Aplicaciones: identificación de vulnerabilidades y riesgos, verificación del cumplimiento normativo, evaluación de la efectividad de los controles.

TERCER AÑO

21 - Amenazas Emergentes y Ciberseguridad

Amenazas en IA, riesgos algorítmicos. Vectores de ataque en IoT. Blockchain: estructura, vulnerabilidades y ataques. Análisis de casos actuales. Seguridad adaptativa y automatizada.

22 - Seguridad en la Nube

Seguridad en la Nube. Contenedores, Docker, Kubernetes. Seguridad en el pipeline DevOps. DevSecOps. Pruebas automatizadas de seguridad. Hardening de microservicios. CI/CD seguro.

23 - Ciberseguridad Industrial y Sistemas Críticos

Ciberseguridad Industrial y Sistemas Críticos (ICS/SCADA). Arquitectura de ICS. Sistemas SCADA, PLCs y redes industriales. Infraestructuras críticas. Riesgos y ataques conocidos. Normativas sectoriales (ISA/IEC 62443, TISAX). Protección, monitoreo, detección y respuesta en entornos industriales.

24 - Ética y Deontología Profesional

Fundamentos éticos (Aristóteles, Kant, utilitarismo). Responsabilidad, praxis y conciencia social. Diseño sustentable, ético y accesible. Propiedad intelectual, competencia leal, contratos, derechos y valores universales. Ética profesional en ciberseguridad. Marco regulatorio. Implicaciones sociales y de privacidad.

25 - Práctica Profesionalizante 3

Auditoría en Comercio Electrónico/Entornos Industriales: identificación de vulnerabilidades y riesgos, verificación del cumplimiento normativo, evaluación de la efectividad de los controles.



Mgter. Jorge Omar Abel Jaimez
Secretario Académico y de Posgrado
Universidad Provincial de Córdoba

ES COPIA
DEL ORIGINAL

26 - Seguridad en Comercio Electrónico

Protocolo HTTPS. Certificados SSL/TLS. Autenticación multifactor. Seguridad en medios de pago. MFA. Prevención del fraude. PCI-DSS. Protección de datos financieros. Normativas y cumplimiento.

27 - Ciberdefensa, Ciberinteligencia y Guerra Cibernética

Estrategias de ciberdefensa estatal y privada. Amenazas persistentes avanzadas (APT). Hacktivismo. Guerra cibernética. Inteligencia de amenazas (Threat Intelligence). Técnicas OSINT. Modelos de colaboración internacional.

28 - Ciberseguridad para Fuerzas de Seguridad y Organismos Públicos

Contenidos mínimos: Rol del Estado en la protección digital. Preservación de evidencia digital. Amenazas globales y delitos complejos. Tareas investigativas en ciberdelitos. Seguridad pública, articulación interagencial y protocolos de intervención. Formación especializada para fuerzas de seguridad y justicia.

29 - Práctica Profesionalizante 4

Elaboración de un protocolo ante vulneraciones y riesgos digitales: recursos necesarios, diseño de nuevos instrumentos de seguridad y estrategias de trabajo para su implementación.

Práctica Profesional Supervisada (PPS). Aplicación e integración para la resolución de situaciones concretas. Evaluación integral de riesgos, defensa, cumplimiento y auditoría. Redacción técnica y presentación oral.

3.4. Propuesta de seguimiento curricular

El/la responsable académico/a de la carrera estará a cargo de la organización y gestión de la tecnicatura, con el fin de alcanzar los objetivos y el perfil profesional propuesto. Asimismo, será responsable del seguimiento e implementación del plan de estudios y de su revisión periódica. Tendrá injerencia en acciones de gestión académica como la conformación de equipos, cumplimiento de los programas de las asignaturas, seguimiento de la formación teórica y práctica brindada a los estudiantes, métodos de enseñanza y formas de evaluación, entre otros aspectos.

