Resolución CS - 142 / 2024

JOSÉ C. PAZ, 05 de noviembre de 2024

VISTO

El Estatuto de la UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ aprobado por Resolución del MINISTERIO DE EDUCACIÓN Nº 584 del 17 de marzo de 2015, la Resolución CS Nº 97 del 13 de julio de 2018, la Resolución CS Nº 177 del 26 de diciembre de 2023, la Resolución Rectoral Nº 402/2024, el Expediente Nº 876/2024 del Registro de esta UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ, y

CONSIDERANDO:

Que mediante la Resolución CS Nº 97 del 13 de julio de 2018 se aprobó el REGLAMENTO DE GESTIÓN ACADÉMICA PARA EL DISEÑO, SEGUIMIENTO Y EVALUACIÓN DE PLANES DE ESTUDIOS DE LAS CARRERAS DE GRADO Y PRE GRADO, en cuyo artículo segundo, primer párrafo establece que "En el mismo acto de creación de la nueva Carrera de Grado o Pre-grado el CONSEJO SUPERIOR DE LA UNPAZ le encomendará al RECTORADO la conformación de una Comisión Técnica para el Diseño del Plan de estudios de la Carrera, que estará integrada por tres (3) docentes/investigadores/as de reconocida trayectoria en el área disciplinar correspondiente, y que serán propuestos por el CONSEJO DEPARTAMENTAL en el que se haya encuadrado la Carrera".

Que mediante la Resolución CS Nº 177 del 26 de diciembre de 2023 se creó la Carrera de TECNICATURA UNIVERSITARIA EN REDES Y SEGURIDAD INFORMÁTICA dentro del ámbito del DEPARTAMENTO DE ECONOMÍA, PRODUCCIÓN E INNOVACIÓN TECNOLÓGICA de esta Universidad.

Que mediante la Resolución Rectoral Nº 402/2024 se conformó la Comisión Técnica para el Diseño del Plan de Estudios de la Carrera de TECNICATURA UNIVERSITARIA EN REDES Y SEGURIDAD INFORMÁTICA.

Que como consta en las actuaciones de la referencia, la Comisión Técnica elaboró el mencionado Plan de Estudios.

Que el CONSEJO DEPARTAMENTAL DE ECONOMÍA, PRODUCCIÓN E INNOVACIÓN TECNOLÓGICA, tal como consta en el Acta Nº 48 de la Sesión del mismo número de fecha 08 de octubre de 2024, ha tomado la debida intervención conforme a las competencias que le fueron otorgadas mediante el artículo 77 inciso e) del Estatuto de la UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ.

Que la SECRETARÍA ACADÉMICA ha tomado su debida intervención.

Que la SECRETARÍA GENERAL y la DIRECCIÓN DE ASUNTOS JURÍDICOS, dependiente de la SECRETARIA LEGAL Y TÉCNICA han tomado la intervención de acuerdo a su competencia.

Que la presente medida se adopta en ejercicio de las atribuciones conferidas por el inciso g) del artículo 63 del Estatuto de la UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ, aprobado por Resolución del entonces MINISTERIO DE EDUCACIÓN nº 584/15.

Por ello,

EL CONSEJO SUPERIOR DE LA

UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ

RESUELVE:

ARTÍCULO 1°.- Apruébase el Plan de Estudios de la carrera de TECNICATURA UNIVERSITARIA EN REDES Y SEGURIDAD INFORMÁTICA que como anexo forma parte de la presente medida.

ARTÍCULO 2°.-Regístrese, comuníquese, publíquese en el Boletín Oficial de la UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ y cumplido, archívese.

Lic. Santiago Mónaco
Secretario
CONSEJO SUPERIOR

Abog. Darío Kusinsky
Presidente
CONSEJO SUPERIOR

Archivos adjuntados

Nombre del archivo
EXP_876-2024_ANEXO_I_(Plan_de_Estudios_Tec._Univ._Redes_y_Seguridad_Informa_tica).pdf

ANEXO

DEPARTAMENTO DE ECONOMÍA, PRODUCCIÓN E INNOVACIÓN TECNOLÓGICA

Plan de estudios de la Tecnicatura Universitaria en Redes y Seguridad Informática

1. Nombre de la carrera:

Tecnicatura Universitaria en Redes y Seguridad Informática.

2. Título/s que otorga:

Técnico/a Universitario/a en Redes y Seguridad Informática.

3. Carga horaria total:

1376 horas.

4. Modalidad de cursada:

Presencial.

5. Requisitos de ingreso:

Poseer título de nivel secundario, o bien ser mayor de 25 años sin título de educación secundaria, y completar los requerimientos establecidos en el artículo 7° de la Ley N° 24.521 y en la normativa institucional correspondiente.

Haber completado el Ciclo de Inicio Universitario (CIU), o bien cumplir con los requisitos para la eximición del CIU establecidos en la normativa institucional correspondiente.

6. Unidad académica de gestión de la carrera:

Departamento de Economía, Producción e Innovación Tecnológica.

7. Fundamentación del proyecto:

En la era digital actual, los desarrollos informáticos se han convertido en pilares fundamentales en el ámbito de la tecnología de la información para el funcionamiento eficiente de organizaciones y de la sociedad en su conjunto. En este contexto, las redes informáticas definen estructuras interconectadas que permiten la comunicación y el intercambio de información entre dispositivos electrónicos, y facilitan el acceso a recursos en entornos digitales. En forma transversal al campo informático, la seguridad informática comprende una disciplina conformada por prácticas, políticas y tecnologías diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información almacenada en sistemas informáticos.

Comprender la naturaleza de los fundamentos de las redes de datos y su relación con la seguridad informática es esencial para abordar los desafíos tecnológicos contemporáneos. Es por ello que la creación de esta propuesta formativa es distintiva en el territorio ya que contempla dos áreas de estudio íntimamente relacionadas; las redes de datos y la seguridad informática integradas en un mismo plan de estudio con la finalidad de formar profesionales

hábiles en esta área de demanda técnica profesional.

La estructura curricular está diseñada para integrar asignaturas que abarcan diversas áreas del conocimiento, desde las ciencias y tecnologías básicas hasta otros campos de estudio. Además, incluye un conjunto de contenidos teóricos y prácticos de tecnologías aplicadas comunes entre las propuestas de formaciones tecnológicas de pre grado y grado de esta casa de estudios. En este sentido, la Universidad Nacional de José C. Paz establece acuerdos y convenios con organizaciones públicas, privadas y comunitarias de la región, enfocándose en la innovación y la transferencia tecnológica. Se promueven acciones con pymes y otras entidades provinciales y municipales para impulsar el desarrollo local y nacional. Considerando el potencial de la disciplina para contribuir a este crecimiento, el proyecto contempla la incorporación de prácticas pre-profesionales supervisadas. Estas prácticas permitirán a las y los futuros graduados aplicar los conocimientos adquiridos en un entorno real y contextualizado.

El plan de estudios de la tecnicatura considera las diferentes configuraciones de perfiles profesionales requeridos por las organizaciones del sector al incorporar profesionales técnicos en sus equipos de trabajo. Se busca que las y los graduados posean una visión integral del campo profesional, así como habilidades prácticas específicas para abordar y resolver necesidades tecnológicas particulares. En este sentido, la selección de las asignaturas busca proporcionar a los estudiantes una formación técnica inicial fuertemente focalizada en redes de datos, para luego profundizar en el campo de la seguridad informática. En el primer año, se busca establecer una base sólida en matemáticas, fundamentos de computación y física informática, lo que proporciona una comprensión básica de la estructura interna de los dispositivos de redes y sistemas informáticos. Mediante la incorporación de los fundamentos de programación se introduce a los estudiantes en los conceptos básicos de la escritura de código y el desarrollo de software, que afianzarán hacia el segundo año de la carrera junto con conocimientos de base de datos. En los dos últimos cuatrimestres, el plan de estudio presenta la oportunidad de profundizar aún más en áreas específicas de la seguridad informática y sus aplicaciones. Finalmente, el laboratorio final integrador y la práctica profesional supervisada brindan la oportunidad de trabajar en colaboración con empresas o instituciones del sector, aplicando las habilidades y conocimientos obtenidos a lo largo de la carrera en un entorno laboral real y adquiriendo experiencia valiosa para su futura carrera profesional.

8. Propósitos generales de la carrera:

La carrera Tecnicatura de Redes y Seguridad Informática se propone:

1. Formar profesionales técnicos con sólidos conocimientos, habilidades prácticas y recursos procedimentales para participar en la implementación o mejora de proyectos de redes y servicios tecnológicos relacionados con la seguridad informática.
2. Contribuir a la defensa de la integridad, confidencialidad y disponibilidad de la información que fluye a través de redes interconectadas.
3. Promover una defensa activa del derecho a la información y la inclusión digital, atendiendo a los desafíos actuales y futuros del mundo digital, y a los nuevos desarrollos de las redes de datos y la ciberseguridad.
4. Aportar a la atención de las necesidades en redes y ciberseguridad en ámbitos de orden social, público y privado, contribuyendo al desarrollo local y nacional.

9. Objetivos de la carrera:

Se espera que los y las estudiantes de la carrera Tecnicatura en Redes y Seguridad Informática:

1. Conozcan, comprendan y dominen las tecnologías de interconexión de redes y servicios de seguridad informática, para diseñar, implementar, diagnosticar y mantener redes informáticas y servicios tecnológicos, aplicando medidas de ciberseguridad que garanticen entornos informáticos confiables.
2. Realicen análisis y diagnósticos del estado de diferentes tipos de redes de comunicaciones para su óptima utilización, basándose en los estándares de las tecnologías pertinentes con especial énfasis en los aspectos de arquitectura, implementación e impacto social y organizacional.
3. Dominen, desde el punto de vista defensivo, conocimientos vinculados con la seguridad física, las prácticas criptográficas, el desarrollo de software seguro, la gestión de la seguridad, la ciencia forense informática, las normativas y legislaciones vigentes relacionadas, y la protección de las redes e infraestructuras tecnológicas modernas.
4. Adquieran los conocimientos, habilidades, criterios profesionales y éticos necesarios para insertarse de manera progresiva en espacios organizacionales, aplicando aportes prácticos y formando parte de equipos multidisciplinarios de trabajo en el ámbito de las redes de datos y la seguridad informática.

10. Alcances del título:

Los/as Técnicos/as Universitarios/as en Redes y Seguridad egresados/as de la Universidad Nacional de José Clemente Paz serán capaces de:

1. Diseñar, instalar, administrar, mantener, operar y monitorear redes informáticas de mediana envergadura.
2. Colaborar en la evaluación de la factibilidad, planificación, implementación y despliegue de redes de datos y voz de gran alcance.
3. Participar en la ejecución de medidas, auditorías y procedimientos de ciberseguridad sobre recursos tecnológicos.
4. Colaborar en la proyección, desarrollo e implementación de políticas y normas de Seguridad Informática.
5. Colaborar en el diagnóstico, documentación y búsqueda de soluciones a problemas e incidentes verificados en redes de datos y/o sistemas de seguridad informática.
6. Asistir técnicamente e instruir a usuarios en materia de redes y comunicaciones, como así también en el campo de la seguridad informática.
7. Integrar equipos multidisciplinarios con profesionales de otros campos técnicos informáticos.
8. Participar en el desarrollo de proyectos, productos o servicios tecnológicos de calidad.

11. Perfil del egresado/a:

Los técnicos y las técnicas universitarias en Redes y Seguridad Informática de la UNPAZ

serán profesionales capaces de desempeñarse en campos de trabajo asociados a áreas de Tecnologías de la Información y la Comunicación (TICs) con conocimientos relativos al funcionamiento del software y el hardware de dispositivos. Contarán con habilidades para diseñar, analizar, configurar, mantener y optimizar redes informáticas, así como para implementar acciones de seguridad efectivas en entornos tecnológicos diversos. Poseerán sólidos conocimientos en los aspectos fundamentales de las redes, las comunicaciones informáticas y la seguridad de la información. Podrán identificar necesidades y demandas en diversos sectores relacionados con infraestructuras tecnológicas fortaleciendo el desarrollo de proyectos, productos o servicios.

Estarán en condiciones de definir de manera creativa procedimientos, normas, estándares protocolos y tecnologías de redes de datos y seguridad informática para brindar soluciones técnicas teniendo en cuenta los aspectos de arquitectura, de implementación y de impacto en distintos ámbitos de trabajo con aplicaciones y requerimientos funcionales diversos

Los técnicos egresados y las técnicas egresadas de esta carrera desempeñarán un papel crucial en la protección contra amenazas cibernéticas, contribuyendo a la estabilidad y desarrollo de las organizaciones. Serán profesionales comprometidas/os con el cuidado y la conciencia crítica, y dispondrán de herramientas que habiliten su desarrollo integral en actividades profesionales guiadas por la ética, el compromiso con la verdad y el interés colectivo. Adquirirán las competencias técnicas necesarias para abordar desafíos tecnológicos emergentes vinculados a este campo profesional.

Asimismo, serán profesionales con capacidad de formular y participar en proyectos de redes informáticas en diferentes ámbitos, con la finalidad de desarrollar infraestructuras tecnológicas seguras. Promoverán y concientizarán acerca de las buenas prácticas y el uso adecuado de los recursos tecnológicos facilitando la adopción de estándares abiertos y software libre en los entornos operativos en los que se desempeñan.

Finalmente, los graduados y las graduadas serán competentes para participar en proyectos de transferencia, extensión y vinculación tecnológica relacionadas con el desarrollo tecnológico y la preservación de la información digital.

12. Estructura curricular:

El diseño curricular de esta carrera está compuesto por veinte (20) unidades curriculares (UUCC) organizadas en cinco (5) cuatrimestres, todas de carácter obligatorio para la obtención del título. La estructura curricular ofrece una formación integral y está diseñada para ofrecer un equilibrio entre teoría y práctica, comenzando el trayecto con mayor carga horaria en el aprendizaje de redes y comunicaciones, y avanzando luego en el abordaje sobre el campo de la seguridad informática, de manera de poder culminar con la integración final en la práctica pre profesional.

Cód	Unidad curricular	Cuatrimestre	Carga horaria		Correlatividades
			Semanal	Total	
PRIMER AÑO					
01	Introducción a las redes y las comunicaciones	I	6	96	-
02	Fundamentos de programación	I	4	64	-
03	Sistemas de computación	I	4	64	-
04	Elementos de matemática	I	4	64	-
Carga horaria total Cuatrimestre I: 288 horas					
05	Taller de redes y comunicaciones	II	6	96	1
06	Seguridad de la información	II	6	96	3
07	Inglés técnico	II	4	64	
08	Teoría y física de la comunicación	II	3	48	4
Carga horaria total Cuatrimestre II: 304 horas					
Carga horaria total PRIMER AÑO: 592 horas					
SEGUNDO AÑO					
09	Gestión de la seguridad de la información	III	2	32	6
10	Ciencia, tecnología y sociedad	III	3	48	
11	Gestión de centros de datos	III	6	96	1-3-8
12	Introducción al desarrollo de software	III	4	64	2
Carga horaria Cuatrimestre III: 240 horas					
13	Base de datos	IV	6	96	4-12
14	Ciberseguridad e informática forense	IV	2	32	6-11
15	Criptografia aplicada	IV	4	64	4-6
16	Taller de seguridad en redes	IV	6	96	5-6-11
Carga horaria total Cuatrimestre IV: 288 horas					
Carga horaria SEGUNDO AÑO: 528 horas					
TERCER AÑO					
17	Técnicas para el desarrollo de software seguro	V	3	48	13-15-16
18	Seguridad en infraestructuras	V	2	32	9-11-14
19	Laboratorio integrador	V	6	96	9-13-14-15-16
20	Práctica preprofesional	V	5	80	9-13-14-15-16
Carga horaria total Cuatrimestre V: 256 horas					
Carga horaria TERCER AÑO: 256 horas					
CARGA HORARIA TOTAL TÉCNICO/A UNIVERSITARIO/A EN REDES Y SEGURIDAD INFORMÁTICA: 1376 horas					

13. Contenidos mínimos:

01. Introducción a las redes y las comunicaciones.

Historia y evolución de las redes de computadoras. Introducción al hardware y software de redes computacionales. Modelos/estandarización de las redes, clasificaciones. Modelos de capas físicas, datos, red, transporte y aplicación. Modelos OSI y TCP/IP. Nivel físico: medios de transmisión, cableado estructurado, cable metálico; normas, estándares y certificación. Redes de fibra óptica: normas, estándares y certificación. Redes inalámbricas: normas, estándares y certificación. Nivel de enlace: concepto de enlace, tramas, puentes. Nivel de red: direccionamiento IPv4 / IPv6. Concepto de ruteo, topologías, protocolos IP, resolución de direcciones. Nociones de servicios DHCP, DNS, HTTP, otros. Uso de herramientas y emuladores de red. Diseño, configuración y administración de redes LAN básicas.

02. Fundamentos de programación.

Algoritmos, programas y solución de problemas mediante computadoras. Interpretación vs. compilación. Variables. Expresiones. Sentencias. Estructuras de control de flujo. Tipos de datos. Modularización. Procedimientos y funciones. Parámetros. Vectores y matrices: arreglos unidimensionales y bidimensionales. Procesamiento de archivos.

03. Sistemas de computación.

Sistemas de numeración. Sistema binario, representaciones, sistemas de codificación. Nociones de compuertas y circuitos lógicos. Organización de computadoras. CPU. Memoria. Almacenamiento. E/S. Sistemas operativos, instalación. Nociones de sistemas GNU/Linux. GUIs vs CLIs. Uso de shell, administración y herramientas. Eventos, interrupciones y excepciones. Llamadas al sistema. Administración de recursos, de E/S y archivos. Aplicación de conceptos en diferentes sistemas operativos.

04. Elementos de Matemática.

Lógica de primer orden. Álgebra de Boole: Aplicaciones de la lógica a la programación (estructuras condicionales y expresiones lógicas). Nociones vectoriales aplicadas a la programación. Matrices y operatoria matricial como organización y transformación de datos e imágenes. Conjuntos, relaciones y funciones como modalizadores de situaciones. Casos específicos: funciones exponenciales, logarítmicas y trigonométricas.

05. Taller de redes y comunicaciones.

Arquitecturas de LAN/WAN avanzadas. Nivel de transporte: funciones, protocolos UDP y TCP, multiplexación, concepto de socket, control de congestión. Modelo general de Internet: integración de niveles y protocolos, servicios de red. Ruteo estático y dinámico Encaminamiento, congestión y calidad de servicio. Nivel de aplicación: instalación, despliegue y operación en entornos reales y simulados de servicios de redes y comunicaciones: DNS; TELNET; SSH; FTP; SMTP; MIME; POP; IMAP; HTTP; SMTP, SNMP; SNMPv2, firewalls (gestión de usuarios y control de accesos en un entorno operativo). Gestión de redes VLAN, STP, DHCP. Sistemas autónomos. Sistemas operativos de redes. Monitoreo de redes, protocolo SNMP y formatos de flujo populares: NetFlow, sFlow y JFlow. Conceptos de telefonía IP.

06. Seguridad de la información.

Historia y caracterización del mundo de la ciberseguridad. Escenario global. Principios fundamentales de la seguridad de la información. Tríada CIA. Riesgos IT. Amenazas y vulnerabilidades. Incidentes factores humanos, lógicos y físicos. Protección por capas. CVE,

CVSS. Vectores, técnicas de ataque y mecanismos de defensa. Métricas e indicadores. Introducción a infraestructuras críticas. Servicios y protocolos de seguridad. Exploiting. Hardening. Identidades. Métodos de autenticación. Tendencias de ataques: ingeniería social, phishing, ransomware, suplantación de identidad, 0-day, uso de inteligencia artificial. Seguridad física: áreas seguras y controles de acceso. Medios de seguridad. Respaldo y recuperación de información. Protección de identidad digital y privacidad de datos personales. Roles y perfiles de los profesionales de la ciberseguridad. Ética y cibernética. Gobierno y gestión de la seguridad de la información. Políticas y procedimientos. Planes de concientización y onboarding. Introducción a la gestión de riesgos TI. Nociones de marcos legales regulatorios y normativas generales.

07. Inglés técnico.

Tipología y estructura de textos técnicos y profesionales. Superestructura y macroestructura de textos informativos. Texto y paratexto. Ideas principales y secundarias. Marcadores simples del discurso. Estrategias para la comprensión e interpretación de textos orales y escritos en inglés. Estrategias discursivas para la confirmación o aclaración de contenidos o procesos. Escritura de resumen a partir de textos. Producción oral sintética de textos. Corpus de vocabulario académico. Sistema verbal. Tipología del sistema verbal. Modalidad. Frase nominal. Presentación de desarrollos informáticos.

08. Teoría y física de la comunicación.

Magnitudes físicas. Introducción a la Electrostática: Concepto de corriente eléctrica, resistencia eléctrica y corriente continua. Leyes de Ohm y Kirchoff. Corriente alterna y potencia eléctrica. Nociones de campos magnéticos. Fuentes de campo eléctrico. Ley de Gauss. Potencial electrostático. Fuentes de campo magnético. Ley de Ampere. Inducción electromagnética. Transformadores. Campo electromagnético. Ley de Maxwell. Ondas electromagnéticas aplicadas a redes inalámbricas. Teorema de Shanon. Señales analógicas y digitales. Muestreo. Representación de señales. Nociones de serie de Fourier. Unidades de medidas en telecomunicaciones. Capacidad del canal. Ancho de banda. Nociones de óptica geométrica aplicado a fibra óptica. Nociones de termodinámica, calor y temperatura.

09. Gestión de la seguridad de la información.

Conceptos de auditoría. COBIT. ITIL. Gestión de activos de la información. Evaluación y gestión de riesgos. Gobierno y gestión de seguridad de la información (SGSI). Condiciones legales, marcos regulatorios y normativas generales (ISO Series 27000, CIS Control , NIST Cybersecurity Framework -CSF- and NIST SP 800-53, PCI DSS y relacionadas). Gestión estratégica de la seguridad en una organización. MAGERIT, NIST SP 800-30, ISO 27005. Herramientas y organización de la información. Controles y auditoría. Informes técnicos y ejecutivos. Gestión de incidentes: metodologías y respuesta. Plan de respuesta a incidentes. Auditorías de seguridad de la información. Auditorías certificables de un SGSI. Auditoría sobre controles de seguridad. ISO 27007. Sistema de gestión de la continuidad del negocio (BCMS). Plan de recuperación ante desastres (DRP). ISO 22301.

10. Ciencia, tecnología y sociedad.

Ciencia, tecnología, industria y desarrollo. Caracterización de la industria tecnológica. El método científico. Investigación, desarrollo, innovación y transferencia. Tecnologías de la información y la comunicación, concepto, historia y evolución. Modos de producción de software. Software libre. Perfiles profesionales y roles informáticos en la actualidad.

Profesionales de ingeniería, telecomunicaciones, software, ciberseguridad, e inteligencia artificial. Impacto social de las producciones de estos campos en las dimensiones económicas, legales, ambientales, entre otras. La innovación tecnológica en el mundo del trabajo: proceso de trabajo, relaciones laborales, rol del Estado. Marcos normativos y regulatorios. Casos de estudio. Responsabilidad y ética profesional. Perspectiva de género.

11. Gestión de centros de datos.

Centros de datos. Almacenamiento y procesamiento de información y servicios brindados. Aspectos de diseño y construcción de un datacenter. Arreglos RAID. Caracterización de computación en la nube. Virtualización. Hipervisores. Tipos de virtualización. Entornos de administración de máquinas virtuales. Contenedores. Nociones de infraestructura como código. Tecnologías como servicios. Especificación, proyecto y desarrollo de la red de datos. Nociones de redes definidas por software SDN. Esquemas de copias de respaldo y consideraciones de seguridad física.

12. Introducción al desarrollo de software.

Introducción a sistemas GNU/Linux. Manejo de terminal y comandos básicos. Nociones de entornos de programación. Depuración. Control de versiones. Conceptos de arquitectura de software en capas, backend, frontend. Nociones de bases de datos. Nociones de desarrollo web, HTML, CSS, Javascript. Framework, concepto y utilización en el desarrollo de software. Concepto y uso de interfaces de programación de aplicaciones. Nociones de despliegue de aplicaciones.

13. Base de datos.

Propósito de las bases de Datos. Modelos de datos. Modelo Relacional. Diagramas entidad-relación. Diseño de bases de datos relacionales. Normalización. Sistemas de Gestión de Bases de Datos Relacionales. Álgebra relacional. Lenguaje SQL. Lenguajes de Descripción, Manipulación y Control de Datos. Transacciones. Concurrencia. Bases de datos no relacionales, clave-valor, documentos, objetos y grafos. Sistemas de gestión de bases de datos no relacionales. Gestión de la información.

14. Ciberseguridad e informática forense.

Cibercrimen. Análisis forense. Evidencia digital, investigación, adquisición de pruebas, cadena de custodia y protocolos de actuación. Documentación. Dictámenes del perito e investigador. Imágenes forenses y *hash* de evidencia digital. *Sandbox*. Análisis de dispositivos móviles y nube. Estándares. Marco normativo, legislación y código de derecho de la ciberseguridad. Preservación de la privacidad y protección de datos personales. Derechos digitales. Prevención y actuación sobre el ciberdelito. Autoridades y gestión de trámites ante CSIRT & CERT. Unidades fiscales, fuerzas federales y locales.

15. Criptografia aplicada.

Introducción a la criptografía. Aplicaciones. Antecedentes históricos. Fundamentos matemáticos: teoría de grafos, aritmética entera, divisibilidad, alfabetos y autómatas. Física y mecánica cuántica. Cifradores de flujo y de bloque. AES. Esquema de cifrado asimétrico y simétrico. Diffie-Hellman, RSA. Funciones Hash. SSL/TLS. Esquema de firma digital. PGP. Esteganografía. Certificado digital. Infraestructura de claves públicas. *Blockchain*, *wallets* y firmas digitales. Dinero electrónico. *Ecommerce*. Protocolos de seguridad. Servicios de identidad, autenticación segura y biometría. Nociones de cifrado cuántico.

16. Taller de seguridad en redes.

Instalación, despliegue y operación en entornos reales y simulados de mecanismos de protección: *firewalls* NG, IDS e IPS, HIDS y *honeypots*. Antivirus tradicionales y EDR. Redes y modalidades: VPN. Ipsec. Seguridad inalámbrica. Protocolos de autenticación. Ataques dirigidos a las características de los protocolos TCP/IP. Seguridad en el servicio de email. Seguridad en la Web. Robo de rutas BGP y ataques de MITM. Ataques de DDoS. Protección de websites. Anonimato en redes. Técnicas de descubrimiento, scanning, sniffing. Herramientas y análisis de muestras de tráfico. Herramientas de gestión de eventos e información de seguridad SIEM. Seguridad en la transmisión de la información. Protocolos seguros: SSH, SFTP, HTTPS. Seguridad en IPv4 e IPv6.

17. Técnicas para el desarrollo de software seguro.

Metodologías, desarrollo y calidad en la ingeniería de software. Seguridad en el software. Vulnerabilidades de los sistemas, ataques. Seguridad de aplicaciones web. Ciclo de desarrollo seguro. Técnicas en el desarrollo seguro de aplicaciones. OWASP Project - OWASP Top 10. CEW top 25 Arquitectura segura. Herramientas de análisis de código. Herramientas SAST vs DAST. Técnicas de análisis de código. Evaluación de amenazas (*Threat Intelligence*). Tipos de *pentesting*. Estrategias de *bug bounty*, uso de *honeypots*. Uso seguro de deep web. Ransomware as a service.

18. Seguridad en infraestructuras.

Servidores. Virtualización: emulación, contenedores. La nube. Modelos: SaaS, PaaS, IaaS. Internet de las cosas. Seguridad en la nube. Normativas, directrices y código de buenas prácticas. Normativas ISO 27017 e ISO 27018. Características de la seguridad en *cloud services*. Infraestructuras críticas y ciberseguridad industrial. Normativa ISO 27017. Norma ISO 27018: protección de SCADA. Seguridad en Industria 4.0. Normativa general y específica sobre seguridad multidimensional y ciberseguridad en infraestructuras críticas. Estrategias de defensa. Estándares ISA 99/IEC 62443, NIST 800-82. Servicios *cloud* y gestión de autenticación y autorización.

19. Laboratorio integrador.

Trabajo en laboratorio: observación, análisis, exploración, diagnóstico, y solución de incidentes de ciberataques y otros problemas del campo en escenarios situacionales simulados. Formalización y documentación de problemas. Sistema de prácticas y tecnologías para estimación de exposición, test de penetración, gestión y tratamiento de vulnerabilidades. Tipos de informes y análisis. Tácticas, técnicas y procedimientos defensivos y ofensivos. Red Red Team y Blue Team. Búsqueda de exploits para acceso inicial y escalamiento de privilegios. *Buffer overflow. Fuzzing*. Acciones post explotación. Estudios forenses y de logs. Explotación y defensa de la red e ingeniería inversa.

20. Práctica pre profesional.

Desempeño supervisado en distintos ámbitos del campo profesional laboral. Análisis y producción de documentación e informes técnicos, versionado. Habilidades de comunicación, organización, trabajo en equipo y otras habilidades blandas en ámbitos laborales. Características y dinámicas de la organización empresarial.

Ámbitos de práctica: internos a la universidad (secretarías, departamentos académicos, institutos de investigación, laboratorios u otras dependencias) o externos (organismos y empresas de gestión pública o privada del sector informático o áreas de sistemas y/o TICs en organismos y empresas nacionales e internacionales).

Hoja de firmas

Sistema: sudocu
Fecha: 05/11/2024 13:04:11
Cargado por: ROMINA MAROLT

Sistema: sudocu
Fecha: 06/11/2024 15:12:22
Autorizado por: SANTIAGO MONACO

Sistema: sudocu
Fecha: 16/11/2024 09:17:33
Autorizado por: DARIO EXEQUIEL KUSINSKY