Resolución de Consejo Directivo **712 / 2024 - EXA -UNSa**
EXP. 170/2022 EXA UNSa Dr. SERGIO ROCABADO eleva programa de la asignatura "OPTATIVA III: CIBERSEGURIDAD" de la Carrera Licenciatura en Análisis de Sistemas (Plan 2010).
De: EXACTAS-Dirección de Alumnos

Salta,
09/10/2024

VISTO: La presentación efectuada por el Dr. Sergio Rocabado, solicitando la aprobación del Programa, Régimen de Regularidad y Promoción de la asignatura "Optativa III CIBERSEGURIDAD" de la Carrera Licenciatura en Análisis de Sistemas (Plan 2010).

CONSIDERANDO:

Que, el citado Programa, Régimen de Regularidad y Promoción, cuentan con la opinión favorable del Departamento de Informática, y de la Comisión de Carrera de Licenciatura en Análisis de Sistemas, todas ellas obrantes en el presente Expediente.

Que, la Comisión de Docencia e Investigaciòn aconseja aprobar el Programa Analítico y el Régimen de Regularidad y Promoción.

Que, el Consejo Directivo en su 14° Sesión Ordinaria del 21 de Agosto del 2024, aprobó por unanimidad el despacho de Comisión de Docencia e Investigación.

Que, por Res. D. N° 860/2024 - Exa - UNSa., se dispone que la Sra. Vicedecana de esta Facultad. Dra. María Rita Martearena, asuma funciones directivas de Decanato, por ausencia del Sr. Decano. Mag. Gustavo Daniel Gil;

Que, el Estatuto de la Universidad Nacional de Salta en el Artìculo 113 inciso 8, entre los deberes y atribuciones que le confiere al Consejo Directivo, incluye" *aprobar los programas Analíticos y la reglamentación sobre el Régimen de regularidad y promoción propuesto por los módulos Académicos".*

POR ELLO, y en uso de las atribuciones que le son propias:

EL CONSEJO DIRECTIVO DE LA FACULTAD DE CIENCIAS EXACTAS

R E S U E L VE:

ARTICULO 1.- Aprobar el programa Analítico, el Régimen de Regularidad y Promoción de la asignatura "OPTATIVA III: CIBERSEGURIDAD" de la Carrera de Licenciatura en Análisis de Sistemas (Plan 2010), que como Anexo forma parte de la presente Resolución.

ARTICULO 2.- Notifiquese fehacientemente al Docente responsable de la asignatura "Optativa III: CIBERSEGURIDAD", Dr. Sergio Rocabado. Hágase saber con copia a la Comisión de Carrera de Licenciatura en Análisis de Sistemas, al Departamento de Informática, a la Secretaría de Coordinación Institucional, a la Secretarìa Académica y de Investigación, a la Dirección de Mesa de Entrada Archivo y Digesto, a la Dirección de Alumnos, para su toma de razón, registro y demás efectos. Publíquese en Boletín Oficial. Página web de la Facultad, Cumplido. Archivese.

FJAA/PDO

Esp. Alejandra Paola del Olmo
Secretaria de Coordinación Institucional
Facultad de Ciencias Exactas - UNSa

UNIVERSIDAD NACIONAL DE SALTA
Facultad de Cs. Exactas

Dra. MARÍA RITA MARTEARENA
VICEDECANA
FACULTAD DE CS. EXACTAS - UNSa

ANEXO RES. CD 712/2024 – EXP. N° 170/2022

Asignatura: Optativa III – CIBERSEGURIDAD

Carrera: Licenciatura en Análisis de Sistemas (Plan 2010)

Fecha de presentación: 09/08/2024

Departamento o Dependencia: Departamento de Informática

Cuerpo Docente:

Profesor: Dr. Sergio Rocabado

Jefe de Trabajos Prácticos: C.U. Miguel Aguirre

Modalidad de dictado: Cuatrimestral.

Ubicación en el plan de estudios: La asignatura Optativa III se dicta en el segundo cuatrimestre de quinto año de la Carrera Licenciatura en Análisis de Sistemas, plan de estudios 2010 (resolución CS N° 135/2010 y su modificatoria CS N° 262/2012).

Objetivos de la asignatura:

- Presentar los conceptos básicos relacionados con Ciberseguridad y el uso seguro de las tecnologías de la información.
- Explicar detalladamente las ciberamenazas existentes, evaluando los riesgos y consecuencias de un ciberataque, para que el estudiante comprenda la importancia de la Ciberseguridad en una organización.
- Revisar los aspectos fundamentales de la seguridad informática.
- Estudiar herramientas y mecanismos de seguridad para proteger infraestructuras críticas que procesan, almacenan o transmiten la información digital de una organización.

Desarrollo del programa analítico:

Unidad 1.- Introducción

Seguridad. Activo. Vulnerabilidad. Amenaza. Ataque. Riesgo. Evaluación y gestión. Impacto. Ciberespacio. Ciberseguridad. Ciberamenaza. Ciberdelincuencia. Ciberdelitos. Consecuencias. Técnicas utilizadas por los ciberdelincuentes. Contramedidas. Gestión de la Ciberseguridad. Equipos de Respuesta a Incidentes de Seguridad. Normas y estándares. Legislación y regulaciones.

Unidad 2.- Fundamentos de Seguridad

Confidencialidad, Integridad y Disponibilidad. Identificación. Autenticidad y autenticación. No repudio. Autorización y Auditoría. Control de acceso. Privacidad y anonimato. Buenas prácticas. Recomendaciones.

Unidad 3.- Herramientas de Seguridad

Seguridad en los servidores. Redundancia y recuperación. Seguridad en los End Points. Seguridad en los dispositivos móviles. Seguridad en los dispositivos IoT.
Protección y reducción de vulnerabilidades en los Sistemas Operativos. Gestión de parches y actualizaciones. Controles de acceso y permisos. Backup y Recuperación.
Seguridad en Redes y Comunicaciones. Criptografía simétrica y asimétrica. Hashing. Protocolos de seguridad (SSL/TLS). PKI (Public Key Infraestructure) Firewalls, IDS/IPS. Seguridad en redes inalámbricas. VPN (Virtual Private Network). Seguridad en la Nube.
Análisis de vulnerabilidades. Herramientas y Técnicas. Pruebas de Penetración. Mitigación.

ANEXO RES. CD 712/2024 – EXP. N° 170/2022

Desarrollo del programa de Trabajos Prácticos:

TP N°	Temas	Horas asignadas
1	Casos de Estudio y Análisis de Incidentes: Ejemplos de incidentes recientes y cómo se gestionaron. Impacto de los Ciberataques en la Sociedad y la Economía: Discusión sobre las implicaciones más amplias de los ataques cibernéticos.	4
2	Taller de herramientas de Sniffing y Scanning. Whireshark. Nmap. Portscan. Whois. Sitereport. Robtext.	4
3	Confidencialidad. Implementación de discos con encriptación en tiempo real. Integridad. Publicación de información asegurando la integridad mediante compendios MD5 y SHA	4
4	Protección y endurecimiento (hardening) de entornos Linux/Windows.	6
5	Tolerancia a fallos a nivel disco. Configuración de RAID 5. Redundancia de Servidores	8
6	Implementación de una PKI. Gestión de certificados digitales. Firma digital.	4
7	Protocolos Seguros: HTTPS. Implementación de un Sitio Web Seguro FTPS. Implementación de un servidor FTP seguro	6
8	Implementación de una VPN utilizando certificados digitales y el protocolo SSL/TLS. (OPENVPN)	6
9	Aseguramiento del perímetro. Firewall PFSENSE	6
10	Seguridad WiFi. Acceso a redes WiFi con autenticación RADIUS. FreeRADIUS.	6
11	Análisis de vulnerabilidades en casos simulados.	6
	TOTAL	60

Metodología y Descripción de las actividades teóricas y prácticas:

El dictado de la asignatura está organizado en base a exposiciones teóricas y clases prácticas. En las clases teóricas se brindan a los alumnos los conocimientos necesarios para ser aplicados durante el desarrollo de los trabajos prácticos en laboratorio.

Las clases teóricas se desarrollan utilizando técnicas de exposición visual (diapositivas) que posibilitan una presentación lógica, ordenada y dinámica de cada tema, con vinculaciones a temas precedentes (si las hubiera) y realizando una síntesis de lo expuesto al final de cada tema.

En los casos que resulten adecuados, de acuerdo al contenido de la unidad y con la finalidad de aplicar los conocimientos teóricos adquiridos, se realizan trabajos prácticos en un laboratorio de informática equipado con software de emulación y virtualización. Los alumnos son supervisados y guiados con el fin de lograr un resultado satisfactorio en las prácticas de laboratorio y en la presentación de sus informes.

Se establece el uso de una plataforma educativa en línea basada en entorno Moodle, la cual permite interactuar con los alumnos a través de foros (consultas y novedades), publicar material relacionado con la materia (contenidos, reglamento interno, transparencias, apuntes teóricos y trabajos prácticos) y realizar un seguimiento de las actividades de cada alumno.

Bibliografía principal:

- CYBERSECURITY ESSENTIALS. Charles J. Brooks. John Wiley & Sons 1th ed. 2018. ISBN: 9781119362395
- COMPUTER SECURITY: PRINCIPLES AND PRACTICE. William Stallings & Lawrie Brown. Pearson, 5th Edition. 2023. ISBN: 9780138091712

Bibliografía complementaria:

- NETWORK SECURITY ASSESSMENT Chris McNab. O'Reilly, 3th ed. 2017. ISBN-13: 978-1491910955.
- LINUX SECURITY AND HARDENING. Donald A. Tevault. Packt Publishing. 2018. ISBN-13: 978-1-78862-030-7.
- SEGURIDAD INFORMÁTICA. José Fabián Roa Buendía. McGraw-Hill, segunda edición. 2013. ISBN: 9788448185695
- CASO DE ESTUDIO DE COMUNICACIONES SEGURAS SOBRE REDES MÓVILES AD HOC. Rocabado, Sergio. UNLP 2014. https://doi.org/10.35537/10915/33571

Condiciones de regularización:

Para regularizar la Asignatura, el alumno debe simultáneamente:

- Aprobar cada uno de los dos parciales o sus respectivas recuperaciones, con nota mayor o igual a 60, sobre 100.
- Presentar los trabajos prácticos y laboratorios propuestos por la cátedra.
- Desarrollar un trabajo integrador con el análisis completo de la ciberseguridad de una organización.

Condiciones de aprobación:

En el examen final, el alumno regular es evaluado desarrollando dos temas del programa, los cuales son seleccionados aleatoriamente. La nota mínima de aprobación es de 4, sobre 10. El alumno libre debe aprobar una primera instancia práctica; la segunda instancia es idéntica a la modalidad aplicada a los alumnos regulares.

Correlatividades:

Para el Cursado:

Regularizadas	Aprobadas
Redes de Computadoras II	Sistemas Operativos. Sistemas de Información. Bases de Datos II.

Para el Examen Final:

Aprobadas
Teoría de la Computación III. Redes de Computadoras II.

Esp. Alejandra Paola del Olmo
Secretaria de Coordinación Institucional
Facultad de Ciencias Exactas - UNSa

UNIVERSIDAD NACIONAL DE SALTA
Facultad de Cs. Exactas

Dra. MARÍA RITA MARTEARENA
VICEDECANA
FACULTAD DE CS. EXACTAS - UNSa