



Universidad Nacional de Salta

FACULTAD DE CIENCIAS EXACTAS

Av. Bolivia 5150 - 4400 - Salta

Tel. (0387)425-5408 - Fax (0387)425-5449

Republica Argentina

SALTA, 7 de Agosto de 2015.

Expte. N°: 19.118/13

RESD-EXA N°: 471/2015

VISTO: la nota que corre agregada a fs. 17 de las presentes actuaciones, por la cual se tramita la aprobación del programa y Régimen de Regularidad de la asignatura Optativa II Seguridad y Protección de la Información, para la carrera de la Tecnicatura Universitaria en Programación (Plan 2012), que se dicta en la Sede Regional Orán; y

CONSIDERANDO:

Que la Comisión de Carrera respectiva, aconseja la aprobación del programa, Régimen de Regularidad y Reglamento de Cátedra de la asignatura antes mencionada.

Que el Departamento de Informática analizó el Reglamento y Régimen de Regularidad de la asignatura Optativa II Seguridad y Protección de la Información, aconsejando la aprobación del mismo.

Que la Comisión de Docencia e Investigación, en su despacho de fs. 28, aconseja favorablemente.

Que en tal sentido, se dio cumplimiento a lo establecido en la RESD-EXA N° 049/2011, resolución homologada por RESCD-EXA N° 135/2011.

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

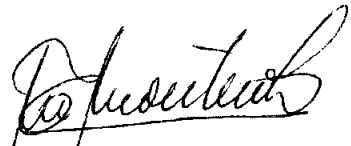
EL DECANO DE LA FACULTAD DE CIENCIAS EXACTAS
(Ad-referéndum del Consejo Directivo)

R E S U E L V E

ARTÍCULO 1.- Aprobar, a partir del período lectivo 2015, el Programa Analítico y Régimen de Regularidad de la asignatura Optativa II Seguridad y Protección de la Información, para la carrera de la Tecnicatura Universitaria en Programación (Plan 2012), que se dicta en la Sede Regional Orán y que como Anexo I, forma parte de la presente Resolución.

ARTÍCULO 2°.- Hágase saber al Ing. Rubén Darío Maza, Departamento de Informática, Comisión de Carrera de Tecnicatura Universitaria en Programación, Departamento Archivo y Digesto y siga a la Dirección de Sede Regional Orán para su toma de razón, registro y demás efectos. Cumplido, archívese.

RGG


Ing. MARÍA TERESA MONTERO LAROCCA
SECRETARÍA ACADÉMICA Y DE INVESTIGACIÓN
FACULTAD DE CS. EXACTAS - UNSa




Ing. CARLOS EUGENIO PUGA
DECANO
FACULTAD DE CS. EXACTAS - UNSa



Universidad Nacional de Salta

FACULTAD DE CIENCIAS EXACTAS

Av. Bolivia 5150 - 4400 - Salta

Tel. (0387)425-5408 - Fax (0387)425-5449

Republica Argentina

ANEXO I - RESD-EXA N°: 471/2015 - Expte. N°: 19.118/13

Asignatura: Optativa II Seguridad y Protección de la Información
Carrera: Tecnicatura Universitaria en Programación (Plan 2012)
Fecha de presentación: 20 de Noviembre de 2013
Departamento o Dependencia: Sede Regional Orán - UNSa
Profesor responsable: Ing. Rubén Darío Maza
Modalidad de dictado: Cuatrimestral

Objetivos de la asignatura:

- a) Presentar los conceptos y técnicas básicas utilizadas para la protección de la información en los sistemas informáticos.-
- b) Adquirir los conocimientos necesarios para aprender a identificar y prever problemas prácticos de seguridad de los sistemas de información, analizando sus vulnerabilidades y las posibles amenazas, y a afrontarlas mediante el diseño e implementación de soluciones.-
- c) Brindar al alumno los conocimientos necesarios para comprender y aplicar métodos y algoritmos criptográficos clásicos y modernos.-

Desarrollo del Programa Analítico

Unidad 1: Introducción

Conceptos básicos. Vulnerabilidad de los Sistemas Informáticos. Amenazas y ataques. Tipos de vulnerabilidad y tipos de amenazas. Contramedidas. Tipos de medidas de seguridad. Objetivos de la seguridad informática. Seguridad física. Seguridad lógica.-

Unidad 2: Código Malicioso

Malware: Definición y clasificación. Virus informáticos: Orígenes y antecedentes. Tipos de virus. Ciclo de vida de un virus. Programas de detección y eliminación de virus. Otros tipos de Malware: Troyanos, Gusanos, Spyware, Hoax, Adware, Ransomware, Bombas lógicas.-

Unidad 3: Criptografía

Definición. Reseña histórica. Métodos Criptográficos. Criptografía Tradicional: Métodos de sustitución y Métodos de transposición. La criptografía y la teoría de la información. Criptografía moderna: Criptografía de clave privada y Criptografía de clave pública. Bases teóricas de la criptografía moderna.-

Unidad 4: Criptografía de Clave Privada

Métodos de cifrado en bloque y Métodos de cifrado en flujo. Modo de operación para sistemas de cifrado en bloque. El estándar para la encriptación de datos (DES): Descripción, Historia, Estandarización.-

Unidad 5: Criptografía de Clave Pública

Criptosistema de Rivest-Shamir-Adleman (RSA). Variante de Rabin-Williams. Sistema de Diffie - Hellman para distribución de claves. Criptosistemas de Merkle - Hellman. Aplicaciones de la Criptografía: Autenticación y Firma digital, Protocolos criptográficos, Criptografía en Internet.-

///...



Universidad Nacional de Salta

FACULTAD DE CIENCIAS EXACTAS

Av. Bolivia 5150 - 4400 - Salta

Tel. (0387)425-5408 - Fax (0387)425-5449

Republica Argentina

-2- ...///

ANEXO I - RESD-EXA N°: 471/2015 - Expte. N°: 19.118/13

Unidad 6: Organización de la Seguridad

Gestión de la seguridad de la información. Políticas, estrategias y normas de seguridad. Análisis de riesgos. Conceptos relacionados con el análisis de riesgo. Planes de contingencia. Seguridad en Redes de Computadoras.-

Desarrollo del Programa de Trabajos Prácticos

T.P. N°	Clases	Tema
1	2	1: Introducción
2	5	2: Código Malicioso
3	5	3: Criptografía
4	5	4: Criptografía de Clave Privada
5	7	5: Criptografía de Clave Pública
6	4	6: Organización de la Seguridad

Bibliografía

- “Aplicaciones Criptográficas” - J. R. Aguirre - Ed. EUI-UPM - 2009.
- “Técnicas Criptográficas de Protección de Datos” - A. Fúster, D. De la Guía, D. Hernández, L. Montoya, F. Muñoz - Ed. Ra-Ma, 1997.
- “Introducción a la Criptografía” - P. Caballero - Ed. Ra-Ma - 2da. Ed. - 2002.
- “Seguridad en Redes Telemáticas” - J. Gallardo Carracedo - Ed. Mc Graw-Hill - 2004.
- “Fundamentos en Seguridad en Redes: Aplicaciones y Estándares” W. Stallings Ed. Pearson Prentice Hall 2003.
- “Seguridad de la Información” - J. Areitio - Ed. Paraninfo - 2008.
- “Criptografía” - A. Maiorano - Ed. Alfaomega - 2009.
- “Enciclopedia de la Seguridad Informática” - A. Gómez Vieites - Ed. Alfaomega - 2007.
- “Criptología y Seguridad de la Información” - P. Caballero, C. Hernández Goya Ed. Ra-Ma - 2000.
- “Protección Informática” - P. Gratton - Ed. Trillas - 1998.-

Metodología y Descripción de las Actividades Teóricas y Prácticas

En las actividades teóricas se impartirán los conceptos teóricos, que servirán de orientación y guía para la “comprensión” de los distintos temas del programa. En el dictado se aplicará la modalidad participativa, con el propósito de que los estudiantes puedan:

///...



Universidad Nacional de Salta

FACULTAD DE CIENCIAS EXACTAS

Av. Bolivia 5150 - 4400 - Salta

Tel. (0387)425-5408 - Fax (0387)425-5449

Republica Argentina

-3- ...///

ANEXO I - RESD-EXA N°: 471/2015 - Expte. N°: 19.118/13

- Plantear sus dudas,
- Realizar preguntas,
- Aportar opiniones,
- Evaluar las contribuciones de sus compañeros, ó incluso,
- Cuestionar lo expuesto por el docente.

También se fomentará que los estudiantes recurran a la bibliografía de diferentes autores para la profundización y maduración de los diferentes conceptos. En tal sentido, y teniendo en cuenta los propósitos generales de la carrera y del programa vigente, se trata de que los alumnos desarrollen:

- El estudio metódico
- El aprendizaje autónomo
- El trabajo colaborativo

Para realizar la exposición de los temas de la asignatura, se utilizarán como recursos fundamentalmente el pizarrón, la computadora y el cañón de proyección, fomentando en todo momento la participación de los alumnos, y tratando fundamentalmente de lograr una fluida comunicación con ellos.

Las actividades prácticas se desarrollarán en el aula y en la sala de computadoras, y consistirán básicamente en la aplicación práctica de los conceptos teóricos, mediante la resolución de problemas en forma individual. Para ello, cada uno de los temas contenidos en el programa dispone de la correspondiente guía de trabajos prácticos, con ejercicios y problemas de complejidad incremental. En la resolución de los problemas planteados se tratará de fomentar el razonamiento y la creatividad de los alumnos, evitando ayudas innecesarias por parte de los docentes. Se resuelven en el pizarrón los ejercicios que sean muy representativos de los conceptos a aplicar, ó que tengan un alto grado de dificultad en su solución.

También se realizarán prácticas de laboratorio, en donde los alumnos:

- Utilizarán y analizarán algunas herramientas de seguridad
- Estudiarán e implementarán algoritmos de cifrado de diversos tipos
- Diseñarán y desarrollarán una aplicación con algoritmos de seguridad

Los alumnos también realizarán actividades prácticas no presenciales, que serán desarrolladas en equipo. Para ello se propondrán trabajos de investigación sobre un determinado tema, trabajos de ampliación en los que se analizarán artículos sobre seguridad informática publicados en revistas especializadas, y el estudio y análisis de casos reales.

Los medios didácticos a utilizar durante el desarrollo de la asignatura comprenden:

- El pizarrón
- El empleo del cañón de proyección de imágenes
- La computadora
- Una guía completa de los Trabajos Prácticos y de Laboratorio
- La sala de computadoras como Laboratorio de Computación para las prácticas en máquina

Sistemas de Evaluación y Promoción

///...



Universidad Nacional de Salta

FACULTAD DE CIENCIAS EXACTAS
Av. Bolivia 5150 - 4400 - Salta
Tel. (0387)425-5408 - Fax (0387)425-5449
Republica Argentina

-4- ...///

ANEXO I - RESD-EXA N°: 471/2015 - Expte. N°: 19.118/13

Se realizaran 2 (dos) Exámenes Parciales, cada uno con su correspondiente recuperación, siendo las condiciones para regularizar la materia las siguientes:

- 75% de asistencia a las clases prácticas.
- 80% de los Trabajos Prácticos y de Laboratorio aprobados.
- Aprobar 2 (dos) Exámenes Parciales o sus correspondientes Recuperatorios, con una calificación mínima de 60 puntos, en una escala de 0 a 100.-

Los alumnos que no Regularicen la asignatura, quedarán en condición de Libres.-

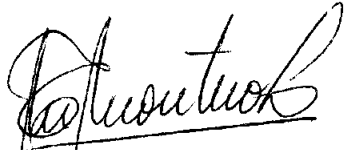
El Examen Final Regular será escrito, y constará de bloques que abarcan el contenido del programa. Para aprobar el mismo deberá reunirse al menos, el 60% del puntaje asignado a cada uno de los bloques.

El Examen Final Libre constará de dos partes:


- La primera parte será de contenido práctico, y para aprobarla deberá reunir como mínimo, el 60% del puntaje asignado a cada uno de los bloques.
- La segunda parte tendrá la misma exigencia que el Examen Final Regular.

La nota final del Examen Final Libre será un promedio de las notas obtenidas en las dos partes aprobadas en las que éste consta.

rgg


M^g. MARÍA TERESA MONTERO LARocca
SECRETARÍA ACADÉMICA Y DE INVESTIGACION
FACULTAD DE CS. EXACTAS - UNSa




ING. CARLOS EUGENIO PUGA
DECANO
FACULTAD DE CS. EXACTAS - UNSa