



Universidad Nacional de Salta  
Sede Orán  
Alvarado N° 751  
Telefax 03878-421388  
\*\*\*\*\*

RESOLUCIÓN N° 027 19

San Ramón de la Nueva Orán, 19 FEB 2019

Expediente N° SO-19.013/19.-

VISTO:

La presentación realizada por el Ing. Rubén Darío Maza, docente de la Carrera Licenciatura en Análisis de Sistemas de la Sede Orán de la Universidad Nacional de Salta; y

CONSIDERANDO:

Que, el Ing. Rubén Darío Maza eleva a consideración de la Comisión de Carrera de la Licenciatura en Análisis de Sistemas, el Programa Analítico de la Asignatura Seguridad y Protección de la Información (Optativa II) del Tercer Año – Segundo Cuatrimestre – Plan de Estudios 2010.-

Que, la presentación realizada se enmarca en el Requerimiento N° 8 del Informe de la CONEAU, sobre el Proceso de Acreditación de la Carrera de la Licenciatura en Análisis de Sistemas.-

Que, toma conocimiento la Comisión de Asuntos Administrativos, Académicos y Presupuestario del Área de Ciencias Exactas de la Sede Orán de la Universidad nacional de Salta, siendo necesario elaborar el instrumento legal correspondiente que avale las presentes actuaciones; y

POR ELLO:

EL VICEDIRECTOR A/C DIRECCIÓN DE LA SEDE ORAN  
DE LA UNIVERSIDAD NACIONAL DE SALTA  
R E S U E L V E

ARTÍCULO 1º: Avalar la presentación realizada por el Ing. Rubén Darío Maza, con relación al Programa Analítico de la asignatura Seguridad y Protección de la Información (Optativa II) del Tercer Año – Segundo Cuatrimestre – Plan de Estudios 2010, de la Carrera Licenciatura en Análisis de Sistemas, que se dicta en la Sede Orán de la Universidad Nacional de Salta, y que se detalla en el Anexo I de la presente resolución.

ARTICULO 2º: Elevar la presente resolución a la Facultad de Ciencias Exactas para su convalidación; y cursar copia a Secretaría Académica de la Universidad, Comisión de Asuntos Administrativos, Académicos y Presupuestario del Área de Ciencias Exactas, Comisión de Carrera, Consejo Asesor y Secretaria de Sede para su conocimiento y efectos.-

hc

LIC. PEDRO E. RUEDA  
SECRETARIO SEDE ORÁN  
UNIVERSIDAD NACIONAL DE SALTA



Prof. EUSEBIO ATANACIO MÉNDEZ  
VICE DIRECTOR SEDE ORÁN  
UNIVERSIDAD NACIONAL DE SALTA



Universidad Nacional de Salta  
Sede Orán  
Alvarado N° 751  
Telefax 03878-421388  
\*\*\*\*\*

RESOLUCIÓN N° 027 19

ANEXO I  
Expediente N° SO-013/19  
Resolución N° SO-027/19

UNIVERSIDAD NACIONAL DE SALTA – SEDE REGIONAL ORAN  
CARRERA: Licenciatura en Análisis de Sistemas  
ASIGNATURA: Seguridad y Protección de la Información (OPTATIVA II)  
PLAN DE ESTUDIOS: 2010  
REGIMEN DE CURSADO: Cuatrimestral  
UBICACIÓN EN EL PLAN DE ESTUDIOS: Tercer año – Segundo Cuatrimestre  
CANTIDAD DE HORAS: 4 hs. Teóricas – 4 hs. Prácticas  
DOCENTE RESPONSABLE: Ing. Rubén Darío Maza

### PROGRAMA ANALITICO

#### **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. Orígenes y antecedentes. Tipos de Malware: Virus, Gusanos, Troyanos, Spyware, Hoax, Adware, Ransomware, Bombas Lógicas, etc. Formas de Prevención. Programas de detección y eliminación. Respuestas ante incidentes del Malware. Últimas tendencias en el mundo del Malware.

#### **Unidad 3: Teoría de Números – Matemática Discreta**

Teoría de Números. Operaciones y propiedades de la congruencia. Conjunto completo de restos. Homomorfismo de los enteros. Inversos en un cuerpo. Conjunto reducido de restos. Función de Euler. Teorema de Euler. Algoritmo Extendido de Euclides. Teorema chino del resto. Raíz primitiva de un cuerpo. Algoritmo de exponenciación rápida.

#### **Unidad 4: Criptografía Clásica**

Fundamentos de la Criptografía. Conceptos básicos de la Criptografía. Principios de la Criptografía y reseña histórica. Fundamentos de las matemáticas discretas para la Criptografía. Sistemas de cifrados clásico. Algoritmos de cifrado por transposición o permutación. Algoritmos de cifrado por sustitución monoalfabética. Algoritmos de cifrado por sustitución polialfabética.





Universidad Nacional de Salta  
Sede Orán  
Alvarado N° 751  
Telefax 03878-421388  
\*\*\*\*\*

ANEXO I  
Expediente N° SO-013/19  
Resolución N° SO-027/19

**Unidad 5: Criptografía de Clave Privada**

Características de los sistemas de encriptamiento modernos. Sistemas simétricos versus sistema asimétrico. Tipos de cifrados simétrico: de flujo y en bloque. Generalidades del cifrado de flujo. Algoritmos de cifrado en bloque: DES, 3DES, IDEA, AES. Modos de operaciones para sistemas de cifrado en bloque.

**Unidad 6: Criptografía de Clave Pública**

Funciones hash. Introducción. Características y propiedades de las funciones hash. Integridad y esquemas de autenticación. Tipos de funciones hash: MD5, SHA-1, SHA-256 y SHA-3. Introducción a los sistemas asimétricos. Intercambio de clave de Diffie-Hellman. El algoritmo RSA. Criptosistema de Rivest-Shamir-Adleman (RSA). El algoritmo de El-Gamal. Aplicaciones de la Criptografía. Autenticación y firma digital. Infraestructura de Clave Pública PKI. Estado legal actual.

**Unidad 7: organización de la Seguridad**

Análisis de riesgo. Definición. Objetivos. Conceptos relacionados con el análisis de riesgos. Metodología. Políticas y controles. Planes de contingencia.

**Programa de Trabajos Prácticos**

T.P. N°	Clases	Tema
1	2	1.- Introducción
2	5	2.- código Malicioso
3	4	3.- Teoría de Números – Matemática Discreta
4	4	4.- Criptografía Clásica
5	5	5.- Criptografía de Clave Pública
6	5	6.- Criptografía de clave Privada
7	3	7.- Organización de la Seguridad

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





Universidad Nacional de Salta  
Sede Orán  
Alvarado N° 751  
Telefax 03878-421388  
\*\*\*\*\*

RESOLUCIÓN N° 027 19

ANEXO I  
Expediente N° SO-013/19  
Resolución N° SO-027/19

- 75 % de asistencia a las clases prácticas.-
- 80 % de los Trabajos Prácticos 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 obtenerse 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.

**Bibliografía Básica**

- Aplicaciones Criptográficas. J.R. Aguirre. Ed. EUI-UPM. 1999.-
- 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. Edición. 2002.-
- Seguridad en Redes Telemáticas. J. Gallardo Carracedo. Ed. McGraw-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.-

**Bibliografía de Consulta**

- Criptografía. A. Maiorano. Ed. Alfaomega. 2009.-
- Enciclopedia de la Seguridad Informática. A. Gómez Vietes. Ed. Alfaomega. 2007.-
- Criptografía y Seguridad de la Información. P. Caballero, C. Hernández Goya. Ed. Ra-Ma. 2000.-
- Protección Informática. P. Gratton. Ed. Trillas. 1998.-

  
LIC. PEDRO E. RUEDA  
SECRETARIO SEDE ORÁN  
UNIVERSIDAD NACIONAL DE SALTA



  
Prof. EUSEBIO ATANACIO MÉNDEZ  
VICE DIRECTOR SEDE ORÁN  
UNIVERSIDAD NACIONAL DE SALTA