FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

RESOLUCIÓN Nº 396

SANTA ROSA, 21de Septiembre de 2018.-

VISTO:

El Expte. Nº 462/18, iniciado por el Mg. Pablo Marcelo GARCIA, docente del Departamento de Matemática s/ eleva programa de la asignatura "Organización de Computadoras II" (Profesorado en Computación – Plan 2014); y

CONSIDERANDO:

Que el docente Mg. Pablo Marcelo GARCIA, a cargo de la cátedra "Organización de Computadoras II", que se dicta para la carrera Profesorado en Computación, eleva programa de la citada asignatura para su aprobación a partir del ciclo lectivo 2018.

Que el mismo cuenta con el aval de la Mg. Silvia BAST, docente de espacio curricular afín, y el de la Mesa de Carreras del Profesorado en Computación.

Que en la sesión ordinaria del día 20 de septiembre de 2018 el Consejo Directivo aprobó por unanimidad, el despacho presentado por la Comisión de Enseñanza.

POR ELLO:

EL CONSEJO DIRECTIVO DE LA FACULTAD DE CIENCIAS EXACTAS Y NATURALES
RESUELVE:

ARTÍCULO 1º: Aprobar el Programa de la asignatura "Organización de Computadoras II" correspondiente a la carrera Profesorado en Computación (Plan 2014), a partir del ciclo lectivo 2018, que como Anexos I, II, III, IV, V, VI y VII forma parte de la presente Resolución.

ARTÍCULO 2º: Regístrese, comuníquese. Dése conocimiento a Secretaría Académica, a los Departamentos Alumnos, de Matemática, al Mg. Pablo Marcelo GARCIA y al CENUP. Cumplido, archívese.

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO I DE LA RESOLUCIÓN Nº 396/18 C.D.

ANEXO I

DEPARTAMENTO: Matemática.

ACTIVIDAD CURRICULAR: Organización de Computadoras II.

CARRERA-PLAN/ES: Profesorado Universitario en Computación - Plan 2014 - Res 446 /14 CS - UNLPam

CURSO: Cuarto Año – Primer Cuatrimestre.

RÉGIMEN: Cuatrimestral.

CARGA HORARIA SEMANAL: 7 hs. **Teóricos:** 4 hs.
Prácticos: 3 hs.

CARGA HORARIA TOTAL: 105 hs.

CICLO LECTIVO: 2018.

EQUIPO DOCENTE: Mg. Pablo Marcelo García (Profesor Adjunto Interino, Dedicación Simple)

FUNDAMENTACIÓN:

Los sistemas operativos han evolucionado notablemente en los últimos años, desde los rudimentarios sistemas basados en intérpretes de comandos e interfaces totalmente textuales hasta las modernas versiones actuales, basadas en lujosas interfaces gráficas, menús contextuales y fuerte base en el concepto de evento.
Similares consideraciones pueden realizarse sobre las redes de computadoras y la comunicación de datos en general, dado que los avances en el hardware y software relacionado con ese punto y otros que resultan accesorios son extraordinarios.
Los sistemas operativos y las redes constituyen un componente de gran importancia en las sociedades modernas y los enormes cambios generados por la evolución de los mismos devienen en una nueva definición de "usuario de computadoras", en todos los niveles.

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO I DE LA RESOLUCIÓN Nº 396/18 C.D.

En consecuencia, la asignatura Organización de Computadoras II se propone presentar los conceptos fundamentales necesarios para la utilización correcta y eficiente de las nuevas posibilidades que los sistemas operativos y las redes de computadoras ofrecen en la actualidad. Se muestran los principios de diseño que permitirán comprender de manera acabada los conceptos que guiarán a la utilización apropiada de los recursos, mostrando en los temas involucrados (por ejemplo, administración de procesos, memoria, archivos, y entrada – salida, compactación, criptografía, criptoanálisis, etc.), ejemplos extraídos de situaciones del mundo real.
La asignatura se basará en las cuestiones conceptuales, pero se verán ejemplos concretos en modelos específicos, tanto en sistemas operativos como en redes.
La evolución de los sistemas operativos ha modificado sustancialmente la manera de relacionarse con las computadoras. Es necesario, en consecuencia, presentar un panorama completo al respecto y promover entre los estudiantes la necesidad de la actualización permanente. Las redes de computadoras, simultáneamente, adquieren una importancia central para los estudiantes de un profesorado en computación.

El nuevo plan de estudios de la carrera (Res. N° 446/14) presenta los siguientes contenidos mínimos:

- Sistemas Operativos. Administración de Procesos.
- Entrada/Salida.
- Administración de Memoria.
- Administración de archivos.
- Redes de computadoras.
- Técnicas de transmisión de datos.
- Modelos.
- Topologías.
- Algoritmos de ruteo.
- Protocolos.
-

Todos esos conceptos exigidos se incluyen en el nuevo programa analítico.

OBJETIVOS Y/O ALCANCES DE LA ASIGNATURA:

El estudiante deberá lograr:

- Incorporar un completo panorama teórico y práctico del manejo de los recursos de un sistema informático por parte de los sistemas operativos (procesos, entrada / salida, archivos y memoria).
- Comprender en profundidad la función que cumple el sistema operativo en lo referente a la relación entre el hardware de una computadora y el software de aplicación que se utilice en la misma.

CORRESPONDE AL ANEXO I DE LA RESOLUCIÓN Nº 396/18 C.D.

- Adquirir conocimientos básicos de los conceptos fundamentales relacionados con las redes de computadoras: técnicas de transmisión de datos, modelos, topologías, algoritmos de ruteo, protocolos, criptografía de llave privada y pública y compactación de la información.

Objetivos específicos

La asignatura se propone transmitir a los estudiantes una visión integral sobre los sistemas operativos y las redes de computadoras.

Los objetivos específicos de la asignatura son:

1. Exponer los conceptos necesarios para la resolución de problemas de concurrencia con la aplicación de semáforos.
2. Presentar las metodologías para la resolución de problemas de concurrencia con la aplicación de Monitores.
3. Exponer las cuestiones relacionadas con la transmisión de información en las redes de computadoras.
4. Aplicar los conceptos basados básicos de la teoría de la información (cantidad de información y entropía).
5. Mostrar las técnicas de compactación entrópica, aplicando los métodos: longitud de series, estadístico y CLUT.
6. Resolver problemas de compactación por fuente, aplicando los métodos: transformaciones, diferencial, y cuantización vectorial
7. Solucionar situaciones prácticas de criptografía y criptoanálisis en base a los métodos de llave privada (César, Vigenere, Beaufort y Vernam) y clave pública (Diffie y Hellman, RSA, El Gamal y Paillier).

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO II DE LA RESOLUCIÓN Nº 396/18 C.D.

ANEXO II

ASIGNATURA/S: Organización de Computadoras II

CICLO LECTIVO: 2018

PROGRAMA ANALÍTICO

Unidad 1: *Sistemas Operativos (S.O.)*

- Introducción. Evolución histórica de los S.O.: Generaciones. Conceptos de S.O.: procesos, archivos, intérprete de comandos. Llamadas al sistema: manejo de procesos, manejo de archivos, manejo de directorios, protección, manejo del tiempo. Estructura de un S.O.: sistemas monolíticos, sistemas en estratos, máquinas virtuales, modelo Cliente - Servidor.
- Administración de Procesos. Modelo. Implementación. Comunicación entre procesos: secciones críticas, exclusión mutua. Bloqueo y desbloqueo. Esquemas basados en multiprogramación: Semáforos y monitores. Problemas clásicos de concurrencia. Planificación de un proceso. Intercambio de mensajes
- Entrada/salida (E/S). Hardware: Dispositivos de E/S. Controladores de dispositivos. Software: Objetivos del software de E/S, manejadores de interrupciones, drivers de dispositivos. Estancamientos: recursos, modelado, detección, recuperación y prevención. Discos: hardware y software. Relojes: hardware y software.
- Administración de la memoria. Monoprogramación. Multiprogramación con particiones fijas y variables. Intercambio. Administración de la memoria con mapas de bits, listas enlazadas y sistema compañero. Distribución del espacio para el intercambio. Análisis de sistemas de intercambio. Memoria virtual: paginación y segmentación. Algoritmos de sustitución de páginas.
- Sistemas de archivo. Aspectos básicos. Directorios. Diseño de un sistema de archivos: manejo del espacio en disco, almacenamiento en archivos, estructura del directorio, archivos compartidos, confiabilidad, rendimiento.

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO II DE LA RESOLUCIÓN Nº 396/18 C.D.

Unidad 2: *Redes de Computadoras*

- Redes de Computadoras. Importancia de las redes informáticas en la sociedad moderna. Hardware: redes de área local, metropolitana, amplia, redes inalámbricas
- inalámbricas y multirredes. Software: Jerarquías de protocolos. Interfaces y servicios. Primitivas de servicios. Relación entre servicios y protocolos. Modelos de referencia: OSI, TCP/IP.
- Modelo Híbrido de redes: capa física. Bases teóricas de la comunicación de datos. Análisis de Fourier. Señales limitadas por el ancho de banda. Tasa de envío máximo de un canal, con y sin ruido. Medios de transmisión: magnéticos, par trenzado, cable coaxial de banda base, cable coaxial de banda ancha, fibra óptica. Transmisión inalámbrica.
- Modelo Híbrido de redes: capa de enlace de datos. Enmarcado. Control de errores. Control de flujo. Códigos de corrección de errores. Códigos de detección de errores.
- Modelo Híbrido de redes: capa de acceso al medio. Problema de reparto de canal. Protocolos de acceso múltiple.
- Modelo Híbrido de redes: capa de red. Diseño. Servicios proporcionados a la capa de transporte. Organización interna de la capa de red. Algoritmos de enrutamiento. Algoritmos de control de congestionamiento. Interredes.
- Modelo Híbrido de redes: capa de transporte. Servicios que proporciona a las capas superiores. Calidad del servicio. Primitivas del servicio de transporte. Elementos de los protocolos de transporte. Direccionamiento. Establecimiento de una conexión. Liberación de una conexión. Control de flujo y buffers. Recuperación de caídas.
- Modelo Híbrido de redes: capa de aplicación. Seguridad de la red. Sistema de nombres de dominio (DNS). Protocolo sencillo de administración de redes (SNMP). Correo electrónico. USENET. World Wide Web.
- Teoría de la Información. Cantidad de información. Entropía. Redundancia. Confusión y Difusión. Transmisión de la información en canales con y sin ruido.
- Compactación. Codificación entrópica: longitud de series, estadística y método CLUT. Codificación por fuente: diferencial, por transformaciones y cuantización vectorial.
- Criptografía clásica: Sustitución y transposición. Procedimientos clásicos de cifrado: César, Vigenere, Beaufort y Vernam.

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO II DE LA RESOLUCIÓN Nº 396/18 C.D.

Condiciones de secreto perfecto de Shannon. Comportamiento de los métodos clásicos de encriptación con respecto al secreto perfecto. Métodos de cifrado en flujo. Generadores seudoaleatorios de secuencia cifrante: período, distribución de ceros y unos, imprevisibilidad, facilidad de implementación.

- Criptografía de clave pública: Diffie y Hellmann, RSA, El Gamal, Paillier.
- Compactación. Codificación entrópica: longitud de series, estadística y método CLUT. Codificación por fuente: diferencial, por transformaciones y cuantización vectorial.

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO III DE LA RESOLUCIÓN Nº 396/18 C.D.

ANEXO III

ASIGNATURA/S: Organización de Computadoras II

CICLO LECTIVO: 2018

BIBLIOGRAFÍA

- **Bacard A.:** "Computer Privacy Handbook" (ISBN 1-56609-171-3). Peachpit Press. 1995.
- **Coutinho S.:** "Números enteros y Criptografía RSA". Instituto de Matemática y Ciencias Afines - Pontificia Universidad Católica del Perú - Universidad Nacional de Ingeniería. ISBN: 99-728-9936-5. 2003.
- **Diffie W., Hellman E.:** "New Directions in Cryptograph", IEEE Trans. Information Theory IT-22 (No. 6, November 1976), pp. 644-654.
- **El Gamal T.:** "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms" IEEE Transactions on Information Theory. Vol 31, ps. 469-472. 1985.
- **Fuster Sabater, A.:** Técnicas Criptográficas de Protección de Datos – Alfaomega Grupo Editor.
- **Lucena López, M.:** Criptografía y Seguridad en Computadores. Segunda Edición. Septiembre de 1999. Departamento de Informática. Escuela Politécnica Superior. Universidad de Jaén.
- **Mao W.:** "Modern Cryptography: Theory and Practice". Prentice Hall - ISBN: 978-0132887410. 2003.
- **McEliece R.:** "A Public Key Cryptosystem Based on Algebraic Coding Theory". DSN Progress Report. 1978.
- **Menezes A., van Oorschot P. and Vanstone S.:** "Handbook of Applied Cryptography". CRC Press. ISBN: 0-8493-8523-7. 1996.
- **Paar C., Pelzl J.:** "Understanding Cryptography: A Textbook for Students and Practitioners". Springer. 2010.
- **Rivest R., Shamir A., Adleman L.:** "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM, Vol. 21 (2), pp.120–126. 1978. Previously released as an MIT "Technical Memo" in April 1977.

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO III DE LA RESOLUCIÓN Nº 396/18 C.D.

- **Shannon C.:** "A Mathematical Theory of Communication". The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656.1948.
- **Stinson D.:** "Cryptography: Theory and Practice". CRC Press. ISBN: 0849385210. 1995.
- **Tanembaun, A.:** Redes de Computadoras – Prentice Hall. 2003.
- **Tanembaun, A.:** Sistemas Operativos – Diseño e Implementación – Prentice Hall. 1999.
- **Tanembaun, A.:** "Sistemas Operativos Distribuidos" – Prentice Hall. 1996
- **Tena J.:** "Protocolos Criptográficos y Seguridad en Redes". Servicio de Publicaciones Universidad de Cantabria. 2003.

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO IV DE LA RESOLUCIÓN Nº 396/18 C.D.

ANEXO IV

ASIGNATURA/S: Organización de Computadoras II

CICLO LECTIVO: 2018

PROGRAMA DE TRABAJOS PRÁCTICOS

Trabajo Práctico 1: *Semáforos.*
Ejercitación destinada a la resolución de problemas de concurrencia con la aplicación de semáforos. Corresponde a la Unidad 1 del Programa Analítico (objetivo específico 1).

Trabajo Práctico 2: *Monitores.*
Ejercitación destinada a la resolución de problemas de concurrencia con la aplicación de Monitores. Corresponde a la Unidad 1 del Programa Analítico (objetivo específico 2).

Trabajo Práctico 3: *Redes de computadoras.*
Ejercitación tendiente a la resolución de ejercicios relacionados con la transmisión de información en las redes de computadoras. Corresponde a la Unidad 2 del Programa Analítico (objetivo específico 3).

Trabajo Práctico 4: *Teoría de la información.*
Este práctico se orienta a la resolución de ejercicios basados en los conceptos de cantidad de información y entropía. Corresponde a la Unidad 2 del Programa Analítico (objetivo específico 4).

Trabajo Práctico 5: *Compactación entrópica.*
Ejercitación cuyo objetivo es la resolución de ejercicios de compactación aplicando los métodos: longitud de series, estadístico y CLUT. Corresponde a la Unidad 2 del Programa Analítico (objetivo específico 5).

Trabajo Práctico 6: *Compactación por fuente.*
Con este práctico se persigue la resolución de ejercicios de compactación aplicando los métodos: por transformaciones, diferencial, y cuantización vectorial. Corresponde a la Unidad 2 del Programa Analítico (objetivo específico 6).

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO IV DE LA RESOLUCIÓN Nº 396/18 C.D.

Trabajo Práctico 7: *Criptografía y criptoanálisis*
Ejercicios con el objetivo de resolver situaciones prácticas aplicando los métodos de César, Vigenere, Beaufort, Vernam, Diffie y Hellman, RSA, El Gamal y Paillier. Criptoanálisis elemental. Corresponde a la Unidad 2 del Programa Analítico (objetivo específico 7).

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO V DE LA RESOLUCIÓN Nº 396/18 C.D.

ANEXO V

ASIGNATURA/S: Organización de Computadoras

CICLO LECTIVO: 2017

ACTIVIDADES ESPECIALES QUE SE PREVÉN: No se prevén actividades especiales.

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO VI DE LA RESOLUCIÓN Nº 396/18 C.D.

ANEXO VI

ASIGNATURA/S: Organización de Computadoras II

CICLO LECTIVO: 2018

PROGRAMA DE EXAMEN

Coincide con el Programa Analítico.

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

CORRESPONDE AL ANEXO VII DE LA RESOLUCIÓN Nº 396/18 C.D.

ANEXO VII

ASIGNATURA/S: Organización de Computadoras II

CICLO LECTIVO: 2018

METODOLOGÍA DE EVALUACIÓN Y/O OTROS REQUERIMIENTOS

Se debe aprobar dos instancias evaluativas o sus correspondientes recuperatorios, existiendo una tercera instancia para uno sólo de ellos. Las fechas de exámenes parciales, recuperatorios y de las exposiciones estarán fijadas en el calendario de la asignatura.