02

JOSÉ C. PAZ, 26 OCT 2020

VISTO:

El Estatuto de la UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ aprobado por Resolución del entonces MINISTERIO DE EDUCACIÓN Nº 584 del 17 de marzo de 2015, el REGLAMENTO DE FUNCIONAMIENTO DEL CONSEJO DEPARTAMENTAL DE ECONOMÍA, PRODUCCIÓN E INNOVACIÓN TECNOLÓGICA, aprobado Resolución del citado CONSEJO N° 01 del 26 de junio de 2020, el Expediente Nro. 201/2020, del Registro de esta UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ, y

CONSIDERANDO:

Que por el Expediente del VISTO tramita la propuesta del programa de la carrera de Licenciatura en Gestión de Tecnologías de la Información correspondiente a la siguiente asignatura: *Seguridad Informática (Cod. 6031).*

Que es competencia de este CONSEJO DEPARTAMENTAL aprobar y supervisar los programas curriculares de las carreras a su cargo, garantizando que aquellos se ajusten a los contenidos mínimos definidos en los correspondientes Planes de Estudios.

UNPAZ

Que habiendo sido puestos a consideración del Consejo DEPARTAMENTAL en la Sesión Nº 19, de carácter ordinaria, registrada en el Acta Nº 19 del 23 de julio de 2020, este Cuerpo Colegiado compartió los términos y contenidos del referido

instrumento, por lo que resulta necesario aprobar el respectivo programa de la asignatura detallada.

Que la presente medida se adopta en ejercicio de las atribuciones conferidas por los artículos 77, inciso f), del Estatuto de la UNIVERSIDAD, y 1°, inciso d) y 7°, inciso c), del Reglamento de Funcionamiento de este Consejo Departamental.

Por ello,

EL CONSEJO DEPARTAMENTAL

DE ECONOMÍA, PRODUCCIÓN E INNOVACIÓN TECNOLÓGICA

DE LA UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ

DISPONE:

ARTÍCULO 1°.- Apruébase el programa de la carrera de Licenciatura en Gestión de Tecnologías de la Información que se adjunta como Anexo a la presente, correspondiente a la siguiente asignatura: *Seguridad Informática (cód. 6031).*

ARTÍCULO 2°.-Establécese que los programas aprobados precedentemente, tendrán DOS (2) años de vigencia, contados a partir del semestre siguiente al de su aprobación.

ARTÍCULO 3°.-Regístrese, comuníquese, publíquese en el Boletín Oficial de la UNIVERSIDAD NACIONAL DE JOSÉ CLEMENTE PAZ y cumplido, archívese.

UNPAZ

02

UNPAZ
Universidad Nacional de José C. Paz

PROGRAMA UNIDAD CURRICULAR

Departamento	**DEPARTAMENTO DE ECONOMÍA, PRODUCCIÓN E INNOVACIÓN TECNOLÓGICA**		
Carrera/s	**Licenciatura en Gestión de la Tecnología de la Información**		
Nombre de la unidad curricular	**Seguridad Informática**	Código	6031
Docente responsable			
Año de presentación del programa	**2019**		

1. Carga horaria

Horas de clase semanales	4		
Horas de clase totales	64	Horas totales clases teóricas	32
		Horas totales clases prácticas	32
		Otras horas totales (laboratorio, trabajo de campo, etc.)	

2. Unidades correlativas precedentes en el Plan de Estudios

Denominación	Código
Laboratorio de Programación y Lenguajes	6014
Programación Orientada a Objetos	6018
Comunicaciones y Redes	6022
Ingeniería de Software II	6027

3. Contenidos mínimos según Plan de Estudios

Fundamentos de seguridad informática. Factores humanos, lógico y físico. Políticas, y procedimientos de seguridad. Área de seguridad informática en una organización. Vulnerabilidades de sistemas informáticos. Arquitecturas de seguridad en sistemas informáticos de organizaciones. Planes de contingencias y continuidad de negocios. Leyes, normas, regulaciones sobre delitos informáticos. Auditoría, peritaje e informática forense.

4. Fundamentación

Seguridad Informática es una unidad curricular que proveerá a sus estudiantes el conocimiento necesario para modelar, implementar, operar, monitorear, revisar, mantener y mejorar continuamente esquemas de gestión de la seguridad de la información.

La continuidad de los procesos de las organizaciones tiene como uno de sus pilares sostener la infraestructura tecnológica que refiere a la captura, procesamiento y obtención de información en sus operaciones. El perfil de Licenciado en Gestión de la Tecnología de la Información debe aprender a comprender los aspectos técnicos y su dinámica en el contexto actual, de forma de poder identificar y gestionar esquemas de seguridad informática.

En ese sentido, se abordan los contenidos esenciales relacionados a la protección de la información vista como uno de los principales activos de las organizaciones.

5. Objetivos

El objetivo general de la unidad curricular es que los estudiantes logren la capacidad de demostrar conocimiento en el campo de la gestión en seguridad de la información, comprendiendo y aplicando los conceptos principales de la seguridad informática y los factores intervinientes en el marco de las problemáticas de las organizaciones, según las leyes, normas y regulaciones vigentes.

Conocimientos a adquirir

- Un conocimiento profundo de los conceptos principales de seguridad de la información y de las tecnologías de ciberseguridad.
- Un conocimiento esencial sobre la teoría y la aplicación de la seguridad de la información en redes informáticas y en el desarrollo del software.
- Un conocimiento profundo sobre la gestión de aspectos vinculados a la seguridad de la información en organizaciones tanto públicas como privadas..

Habilidades a desarrollar

- Integrar conocimientos de las materias correlativas para la comprensión del problema de la seguridad de la información relacionando los aspectos técnicos informáticos con los aspectos de gestión de las organizaciones.
- Aprender a planificar y realizar una investigación guiada limitada basada en la bibliografía de la unidad curricular.
- Comprender la criticidad sobre disponer y evaluar información actualizada relativa a la seguridad de la información y aprender los mecanismos necesarios para su obtención.

- Desarrollar una actitud crítica y reflexiva respecto a la temática de la seguridad informática.

Competencias

- Comprender los objetivos de la seguridad de la información en relación a los activos de una organización, identificando las potenciales amenazas y escenarios de vulnerabilidad.
- Realizar análisis sobre el estado de situación respecto la seguridad informática en una organización.
- Entender los requerimientos de seguridad de la información de una organización, necesidades de políticas y procedimientos.
- Gestionar procesos de implementación y operación de controles respecto de la seguridad de la información.
- Comprender globalmente los aspectos de la seguridad de la información en la industria y los mercados, tanto a nivel técnico como de negocios.

6. Contenidos (organizados por unidades)

UNIDAD 1: Seguridad informática

Seguridad de la información. Terminología. Disponibilidad. Confiabilidad. Integridad. Riesgos, amenazas, vulnerabilidades y ataques. Factores humanos, lógico y físico. Medidas de protección. Plan de continuidad del negocio. Marco de trabajo de seguridad informática.

UNIDAD 2: Seguridad física

Componentes de la seguridad física. Tipos de amenazas a la seguridad física. Seguridad de centros de procesamiento de la información. Controles de acceso. Esquemas de copias de respaldo y recuperación de información.

UNIDAD 3: Seguridad en redes de información

Seguridad de la red. Capa de seguridad de transporte. Seguridad perimetral. Detección y prevención de intrusos. Seguridad en redes inalámbricas. Redes privadas virtuales.
Criptografía. Funciones de hash. Infraestructura de clave pública. Firma digital. Estenografía.

UNIDAD 4: Seguridad en el desarrollo de software

Mecanismos de seguridad en sistemas operativos. Seguridad de aplicaciones. Control de acceso. Esquemas de implementación de autenticación y autorización. Seguridad en aplicaciones web, tipos de vulnerabilidades y medidas de protección.

UNIDAD 5: Gestión de la seguridad informática

Gestión de la seguridad. Políticas. Procedimientos. Áreas de **seguridad informática**. Equipos de respuesta. Centros de operaciones de seguridad. Estándares. **Normas, leyes, regulaciones**. Educación en seguridad informática.

Perfiles profesionales de seguridad informática. Ética y **seguridad informática. Delitos** informáticos. Ley de propiedad intelectual. Ley de Delitos Informáticos. **Auditoría. Peritaje. Forensia** informática.

7. Bibliografía obligatoria y complementaria (organizada por unidades)

UNIDAD 1: Seguridad informática

Bibliografía obligatoria:

- Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. Seventh Edition. Global Edition. Pearson. Capítulo 1.
- Stallings, W., Brown, L. (2018). Computer security: principles and practice, Fourth Edition, Global edition. Pearson. Capítulos 1, 6.
- Barrett, M. P. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework). Capítulos 1 y 2.
- Shirey, R. (2007). RFC 4949: Internet security glossary 2.
- ISO/IEC 27031 (2011). Information technology, Security techniques, Guidelines for information and communication technology readiness for business continuity.
- ISO 22301: (2012). Societal security, Business continuity management systems, Requirements.

Bibliografía complementaria:

- ISO/IEC 27000 (2018). Information technology, Security techniques, Information security management systems, overview and vocabulary.
- Harris, S., & Maymi, F. (2018). CISSP All-in-One Exam Guide, book. McGraw Hill Education.
- Vieites, Á. G. (2011). Enciclopedia de la seguridad informática Grupo Editorial RA-MA.
- Huamán Rivera, O. R. (2018). Diseño de un sistema de gestión de continuidad operativa para una entidad pública bajo el enfoque de la norma ISO/IEC 22301: 2012.
- Wong, W. N. Z., & Shi, J. (2014). Business Continuity Management System: A Complete Guide to Implementing ISO 22301. Kogan Page Publishers.

UNIDAD 2: Seguridad física

Obligatoria:

- Stallings, W., Brown, L. (2018). Computer security: principles and practice. Fourth Edition. Global Edition. Pearson. Capítulos 5, 16,
- Silberschatz, A., Gagne, G., & Galvin, P. B. (2018). Operating system concepts. Tenth Edition. Wiley. Capítulos 11, 14.

Complementaria:

- Telecommunication Industry Association. (2017). TIA-942-B data center standards overview.

UNIDAD 3: Seguridad en redes de información

Obligatoria:

- Stallings, W. (2014). Data and Computer Communications. Tenth Edition. Pearson. Capítulos 13, 14, 23.
- Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. Seventh Edition. Global Edition. Pearson. Capítulos 3, 9, 10, 11, 13, 14, 17, 18.

Complementaria

- Stallings, W., Brown, L. (2018). Computer security: principles and practice. Fourth Edition. Global Edition. Pearson. Capítulos 2, 8, 9, 21, 22, 23 y 24.
- Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. Seventh Edition. Global Edition. Pearson. Capítulo 16.

UNIDAD 4: Seguridad en el desarrollo de software

Bibliografía obligatoria:

- Stallings, W., Brown, L. (2018). Computer security: principles and practice. Fourth Edition. Global Edition. Pearson. Capítulos 3, 4, 5, 11, 12.
- Silberschatz, A., Gagne, G., & Galvin, P. B. (2018). Operating system concepts. Tenth Edition. Wiley. Capítulos 9, 16 y 17.
- STOCK, A. V. D., et al. (2017). OWASP Top 10 2017. The Ten Most Critical Web Application Security Risks.

Bibliografía complementaria:

- Messier, R. (2015). Operating system forensics. Elsevier, Syngress.
- Messier, R. (2019). CEH v10 Certified Ethical Hacker Study Guide. Sybex.

UNIDAD 5: Gestión de la seguridad informática

Bibliografía obligatoria:

- Stallings, W., Brown, L. (2018). Computer security: principles and practice, Fourth Edition, Global edition. Pearson. Capítulos 14, 15, 16, 17, 18, 19.
- Piccirilli, D. (2016). Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia–forensia y cibercrimen).
- Oficina Nacional de Tecnologías de Información (2015). Modelo de Política de Seguridad de la Información para el Sector Público Nacional, Disposición Ministerial 1/15.
- Ley de protección de datos personales, Nº 25.326, 2000.
- Ley de propiedad intelectual, N º 25.036, 1998.
- Ley de Delitos Informáticos - Código Penal, Nº 26.388, 2008.
- Ley de Confidencialidad, Nº 24.766, 1996.

Bibliografía complementaria:

- Himanen, P. (2002). La ética del hacker y el espíritu de la era de la información.
- ISO/IEC (2018). ISO 27000 family of standards for information security management systems.
- Brezinski, D., & Killalea, T. (2002). Guidelines for evidence collection and archiving (RFC 3227).
- Haes, S. D., & Grembergen, W. V. (2016). Enterprise governance of information technology: achieving alignment and value, featuring COBIT 5.
- ISO/IEC 27035-1 (2016). Information technology, Security techniques, Information security incident management, Part 1: Principles of incident management.
- ISO/IEC 27035-2 (2016). Information technology, Security techniques, Information security incident management, Part 2: Guidelines to plan and prepare for incident response.
- Banco Central de la República Argentina (2017). COMUNICACIÓN "A" 6375, Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras.

8. Metodología de trabajo

El desarrollo de las clases estará de acuerdo con criterios que garantizarán el aprovechamiento del

tiempo destinado al proceso de formación, focalizando el tiempo de clase en la comprensión conceptual y desarrollo de las capacidades de aprendizaje de la temática de seguridad, guiando al desarrollo de habilidades prácticas, y fomentando la lectura domiciliaria.

El dictado de las clases se realizará de manera tal que el proceso de enseñanza y aprendizaje permita una efectiva transferencia de conocimientos y comunicación de experiencias relevantes. En las clases se presentarán los temas en exposiciones orales, se harán referencias al material bibliográfico, se realizarán experimentos prácticos y se estudiarán casos reales de aplicación.

En cada clase y cuando lo amerite la correlación de temas, se hará un repaso sintético de los contenidos de la clase anterior y además habrá un espacio con la finalidad de evacuar posibles dudas que los estudiantes posean.

Respecto al cronograma de dictado de clases, la primera clase se realizará la presentación de la unidad curricular y los temas a tratar, y se hará un repaso general del contenido que se toma de las unidades curriculares correlativas. Además, se dictará una clase de repaso de todos los temas tratados en el día de clase previo a examen.

Se complementará el dictado de clases con material disponible en el campus virtual.

9. Evaluación (Requisitos de aprobación y criterios de evaluación)

Evaluaciones parciales

Se proveerán dos instancias de evaluaciones parciales:

Evaluación Parcial I - EXAMEN PARCIAL INDIVIDUAL:

- Evaluación Teórica y práctica. Individual. Presencial, en horario de cursada. De producción escrita.

Evaluación Parcial II - TRABAJO TEÓRICO-PRÁCTICO GRUPAL:

- Evaluación teórica y práctica. Grupal. Domiciliaria (de producción escrita, con posibilidad de entregas parciales) y presencial (de producción oral).

Ambas evaluaciones tendrán una nota correspondiente al esquema de calificación. Estas dos notas serán tenidas en cuenta como base para la aprobación de la Unidad Curricular.

Recuperatorios

Existirá una instancia de recuperación para cada evaluación parcial. A la misma podrán acceder aquellos/as estudiantes que:

- Hayan obtenido una calificación inferior a 7 (siete) puntos.
- Hayan estado ausentes de forma debidamente justificada.

Todas las instancias de recuperación serán individuales, de producción oral y escrita en el caso de la Evaluación Parcial I y de producción escrita en el caso de la evaluación parcial II.

La calificación que los/as estudiantes obtengan en la instancia de recuperatorio reemplazará la calificación obtenida en el examen que se ha recuperado y será la considerada definitiva a los efectos de la aprobación.

Escala de calificación

Todas las calificaciones serán en escala numérica y conceptual, del 1 (uno) al 10 (diez). Los estudiantes podrán solicitar, una vez realizada la calificación, se les de vista y/o una fundamentación explícita del resultado obtenido.

Requisitos de aprobación

Se establecen los siguientes mecanismos de aprobación:

- Mediante promoción directa: quienes hayan obtenido una calificación de 7 (siete) o más puntos como promedio de todas las instancias evaluativas, sean éstas parciales o sus recuperatorios, debiendo obtener una nota igual o mayor a 6 (seis) puntos en cada una de éstas.
- Mediante aprobación de examen integrador: quienes hayan obtenido una calificación entre 4 (cuatro) y 6 (seis) puntos en promedio de las instancias parciales y como mínimo un 4 (cuatro) en cada instancia o en sus respectivos recuperatorios. El examen será de modalidad escrita.
- Mediante examen final: hayan obtenido una calificación entre 4 (cuatro) y 6 (seis) en los

respectivos exámenes parciales y/o sus recuperatorios, pero no hubieren aprobado o asistido a la instancia del examen integrador.

- Mediante examen libre: en aplicación del Régimen de Aprobación en Exámenes Libres.

Criterios de evaluación

Los criterios de evaluación serán en función de los aspectos formales que van a influir en el futuro en el desarrollo de la profesión.

- Por cada punto teórico se evaluará, fundamentalmente, la comprensión y capacidad de reflexión crítica sobre el concepto al que el punto se refiere.
- Por cada punto práctico se evaluará, fundamentalmente, la comprensión del problema a resolver y la formulación de la solución, y en segunda instancia la implementación de la solución.

Por otro lado, se evaluará también la expresión escrita, evaluando la rúbrica y la ortografía de la producción entregada.

10. Instancias de práctica (opcional)

11. Cronograma de actividades teóricas y prácticas

Semana 1	Presentación de la materia. UNIDAD 1: Seguridad informática
Semana 2	UNIDAD 1: Seguridad informática
Semana 3	UNIDAD 2: Seguridad física
Semana 4	UNIDAD 2: Seguridad física
Semana 5	UNIDAD 3: Seguridad en redes de información
Semana 6	UNIDAD 3: Seguridad en redes de información
Semana 7	UNIDAD 3: Seguridad en redes de información UNIDAD 4: Seguridad en el desarrollo de software
Semana 8	UNIDAD 4: Seguridad en el desarrollo de software
Semana 9	Evaluación Parcial I.
Semana 10	UNIDAD 4: Seguridad en el desarrollo de software Instancia de recuperación de la Evaluación Parcial I.
Semana 11	UNIDAD 5: Gestión de la seguridad informática

Semana 12	UNIDAD 5: Gestión de la seguridad informática
Semana 13	UNIDAD 5: Gestión de la seguridad informática
Semana 14	UNIDAD 5: Gestión de la seguridad informática
Semana 15	Evaluación Parcial II.
Semana 16	Instancia de recuperación de la Evaluación Parcial II. Clase de Cierre.

Firma docente responsable	
Firma Departamento Académico