Ministerio de Educación
Universidad Tecnológica Nacional
Facultad Regional Rosario

Rosario, 22 de marzo de 2022.-

VISTO El expediente I.D. N° 8130913 presentado por el Consejo Departamental de Ingeniería en Sistemas de Información, relacionado con el programa analítico de la asignatura electiva "Seguridad en los Sistemas de Información", de la carrera Ingeniería en Sistemas de Información, y

CONSIDERANDO

Que los objetivos y contenidos del mismo se ajustan a la reglamentación vigente.

Que dicho programa cuenta con el aval del respectivo Consejo Departamental.

Que la Comisión de Enseñanza evaluó la presentación y aconsejó su aprobación.

Por ello y atento a las atribuciones otorgadas por el artículo 85° del Estatuto Universitario.

EL CONSEJO DIRECTIVO DE LA FACULTAD REGIONAL ROSARIO
DE LA UNIVERSIDAD TECNOLÓGICA NACIONAL
RESUELVE:

ARTÍCULO 1°.- Aprobar el programa analítico de la asignatura electiva "Seguridad en los Sistemas de Información", que se agrega como Anexo I de la presente resolución, de la carrera Ingeniería en Sistemas de Información a partir del Ciclo Lectivo 2022.

ARTÍCULO 2°.- Establecer que la misma tendrá validez durante cuatro ciclos lectivos consecutivos, según la Ordenanza N° 1383 – Lineamientos para la implementación de asignaturas electivas para las carreras de grado en el ámbito de la Universidad.

ARTÍCULO 3°.- Regístrese. Comuníquese. Cumplido, archívese.

RESOLUCIÓN N° **016**

UTN FRRo
C.D.
S.R.

Ing. Rubén Fernando CICCARELLI
Decano

Ing. Antonio Luis MUIÑOS
Secretario Académico

RESOLUCION N° 016

ANEXO N° 1

Programa analítico de asignatura electiva

Seguridad en los Sistemas de Información

Carrera:	*Ingeniería en Sistemas de Información*						
Departamento:	*Ingeniería en Sistemas de Información*						
Titulación[1]:		*Ingeniería en Sistemas de Información*			*Analista universitario de Sistemas*		
Plan de Estudio:	*2008 – ordenanza 1150*			**Área[2]:**	*Gestión Ingenieril*		
Dictado:		*Anual*	*X*	*Cuatrimestral*	**Nivel:**	**5**	**Electiva:** *Si*
Carga horaria Semanal:	*6*			Carga horaria total de la asignatura:			*96*
Fecha de Confección[3]:	*19/02/2022*			Versión[4]			*9.99*

Fundamentación de la asignatura:[5]	*El programa de la asignatura* ***Seguridad en los Sistemas de Información*** *se concibe dentro de un contexto del objetivo de las incumbencias del título como una ampliación de los conocimientos adquiridos en las cátedras de la carrera de I.S.I. y su enseñanza se debe desenvolver dentro de una concepción didáctica donde el proceso de "enseñanza-aprendizaje" esté centrado en el alumno. Entre el saber y el alumno interviene el docente como mediador-facilitador y esa función de puente entre el alumno -en su tarea de aprendizaje- y el saber existente, es lo que se denomina enseñanza y constituye el ámbito específico de la profesionalidad docente. La enseñanza debe ser útil para el sujeto del aprendizaje, en lo personal actual* (referido a su desarrollo cognitivo y espiritual) *y en lo ocupacional futuro.* *La asignatura* ***Seguridad en los Sistemas de Información*** *tiene como objetivo fortalecer competencias específicas de futuros profesionales de sistemas de información en la materia. La evolución tecnológica y la dependencia creciente de la tecnología en los ámbitos organizacionales y personales exponen a los sistemas de información a riesgos cambiantes y crecientes. Las responsabilidades e incumbencias de un profesional de Ingeniería en Sistemas de Información en cuanto a seguridad y continuidad de negocio de las organizaciones ante la ocurrencia de un evento de seguridad fundamenta los objetivos de la asignatura.*
Objetivos Generales[6]:	*Brindar al alumno las herramientas necesarias para que construyan sus conocimientos en el Área Científico/Técnica/Gestión relacionada con SEGURIDAD EN LOS SISTEMAS DE INFORMACION a través de un marco de referencia ordenado y con prácticas de gestión adecuadas, identificando a su vez la diversidad de recursos y componentes involucrados en la gestión y prevención de riesgos derivados de la tecnología de la información además de la implementación de medidas para prevenir, gestionar e implementar medidas de continuidad de los servicios de tecnología de la Información en constante interacción con las diversas disciplinas que conforman el Plan de Estudio de la carrera, no solo para su desarrollo intelectual sino también para el afianzamiento de sus competencias profesionales.*

[1] *Indique los títulos de la carrera para los que se propone el programa analítico. Márquelos con una cruz.*
[2] *Área a la que pertenece la asignatura*
[3] *refiere a la fecha en que se confecciona o desarrolla la versión*
[4] *Si el programa no es la primera vez que se entrega se produce un cambio en el número de versión cambio. Si el cambio es significativo cambia el entero sino los dígitos después del punto.*
[5] *Importancia para la formación profesional en función del perfil del egresado*
[6] Objetivos generales que justifican la inclusión de la asignatura.

	Proporcionar a los alumnos un enfoque adicional relacionado con el marco regulatorio de la gestión de la tecnología de la información y legislación que regula la protección de datos personales y regulaciones del mercado que exponen al profesional de sistemas en posiciones de dirección a responsabilidades profesionales relevantes en cuanto a seguridad, continuidad y mejores prácticas vinculadas de gestión de la tecnología de la información. *Se orienta hacia la adquisición de competencias intelectuales tales como la capacidad de crítica, de elaboración y de reformulación de las diferentes temáticas a tratar mediante la apropiación de los diversos conceptos, en permanente interacción con el grupo (docente y resto de alumnos), afianzándose el respeto por los derechos propios y de los demás, la autonomía en la toma de decisiones, la valoración de la palabra como manifestación del pensamiento, la confianza en sí mismo y el desarrollo de estrategias de búsqueda de soluciones a las diferentes problemáticas.* *Los objetivos didácticos se basan en la observación, investigación, análisis y estudio, que desarrollarán los alumnos en la compresión de los temas, en constante relación con los conceptos previos (adquiridos en otras cátedras) y en los incorporados durante el desarrollo de esta asignatura.*

Programa de contenido analítico

Programa de contenido analítico

Unidad temática Nº: 1 **UNIDAD 1 – Seguridad de la Información**

Eje Conceptual:

1. **Introducción a la seguridad de los Sistemas de Información.**
2. **Marcos de Gestión de la Seguridad en los Sistemas de información.**

Objetivo/s Específico/s[7]:

Que el alumno tome conocimiento de:

Las amenazas a las que están expuestos los sistemas de información, la legislación y regulación vinculadas con la tecnología para minimizar la exposición a riesgos.
Los diferentes marcos de referencia y estándares vinculados a la seguridad de la información como guía para la gestión y la adaptación a normativas y regulaciones vigentes.
Que en un entorno descentralizado con alto grado de concurrencia de transacciones y usuarios es necesario establecer un marco de control, administración y seguridad.

Temas:

Temas teóricos:

Introducción

Seguridad de la información: definiciones y diferencias: Seguridad informática, seguridad de la información, ciberseguridad.
Triangulo CID : Confidencialidad, Integridad, Disponibilidad
Evolución Tecnológica y efectos en la seguridad
Conceptos de Seguridad Física y Lógica

Gestión de la Seguridad de la Información

Introducción a Sistemas de Gestión de Seguridad de la Información: Políticas de seguridad, Evaluación y administración de riesgos.
Marcos de Referencia y Estándares: COBIT, ITIL, SOX, ISO 27001,.
Legislación,-Normativas y Regulaciones Vigentes en Argentina.
Políticas y Procedimientos de Seguridad de la Información.
Gestión del Riesgos sobre activos de información.

Presupuesto horario teoría: 20 horas

Temas de práctica en laboratorio:

Identificación de riesgos, cuantificación, Confección de matrices de riesgos.

Presupuesto horario práctica: 11 horas

Presupuesto horario total: 31 horas

[7] Objetivos específicos que justifican la inclusión de la asignatura.

Unidad temática N°: 2 : **Seguridad aplicada**
Eje Conceptual:

1. **Proceso de Seguridad de la Información en entornos empresariales.**
2. **Seguridad Física y Ambiental**
3. **Seguridad Lógica**

Objetivo/s Específico/s:

Que el alumno tome conocimientos de:

Las prácticas relacionadas a la mitigación de riesgos y mejores prácticas profesionales en cuanto a Gestión de las Tecnologías de la Información.

La amplitud y diversidad de los riesgos en las Organizaciones y centros de datos corporativos desde la perspectiva física y lógica.

La administración de los servicios, aplicaciones y seguridad en un marco de las prácticas adecuadas de la gestión de tecnología de la información.

Temas:

2.1: Proceso de Seguridad de la Información en entornos empresariales.
Plan de contingencia y continuidad de negocio y recuperación de desastres.
Administración de Usuarios.
Administración y Gestión por Entornos: Desarrollo, testing, Producción. Procesos y buenas prácticas.
Modificaciones e integridad de Bases de datos, Cambios a Programas y puesta en producción.
Estrategias de Backup y Recuperación.

2.2 Seguridad Física y Ambiental.
Centros de datos: Riesgos en Alimentación eléctrica, Refrigeración y Protección contra Incendios – Minimización de Riesgos
2.3 Seguridad Lógica.
Seguridad en Base de datos y Aplicaciones.
2.3.1 Aplicaciones y Software de Base
Seguridad en el desarrollo de aplicaciones. Buenas Practicas.
Segregación de funciones: Desarrolladores, Administradores y Usuarios.
Separación de Ambientes.
2.3.2 Bases de Datos.
Permisos y Privilegios - Roles: Administradores de Base de datos, Desarrolladores, Usuarios de negocios y operativos. Logs de auditoría.

Presupuesto horario teoría: 15 horas

Temas de práctica en laboratorio:

Conceptos comunes a todos los Sistemas Operativos
Valores del Sistema / Lenguaje de Control / Colas de Procesos e Impresiones / Seguridad Física / Niveles de Seguridad / Seguridad de Objetos / Seguridad de Recursos / Resguardo de la información /

Presupuesto horario práctica: 10 horas
Presupuesto horario total: 25 horas

Unidad temática Nº: 3 **Criptografía y Hacking Ético.**

Eje Conceptual:

1. **Conceptos asociados a Criptografía**.
2. **Hacking Ético y Vulnerabilidades**
3. **Identificación de Vulnerabilidades**

Objetivo/s Específico/s:

Que el alumno asocie los principales conceptos de las principales amenazas, consecuencias y alternativas de mitigación a las que están expuestos los sistemas de información en entornos altamente dependientes de la web.

Temas:

3.1 Criptografía.
Conceptos de Criptografía. Algoritmos. Encriptación simétrica y asimétrica. Estrategias. Métodos de autenticación. Autorización.
Firma Digital. Certificados digitales.

3.2 Hacking Ético y Vulnerabilidades
Búsqueda de información - Ingeniería Social - Aplicaciones Web y Core: Evaluaciones de seguridad. Test de Penetración (Pen Testing) – Tipos de ataques y Vulnerabilidades.
3.3: Identificación de Vulnerabilidades: Conceptos Básicos.
Malware – Tipos de Malware – Código Malicioso – Ataques a Correo Electrónico y Aplicaciones

Presupuesto horario teoría: 10 horas

Temas de práctica en laboratorio:

Ejercicios de criptografía e interpretación de requisitos regulatorios vinculados al tema. Revision e interpretación de informes de tests de penetración a organizaciones y recomendaciones de auditorias.

Presupuesto horario práctica: 10 horas
Presupuesto horario total: 20 horas

Unidad temática Nº: 4 **Auditoria Informática y Seguridad.**

Eje Conceptual:

1. **Conceptos de auditoría y control interno – Segregación de funciones**
2. **Metodología de auditoría informática.**

Objetivo/s Específico/s:

Que el alumno adopte las competencias necesarias para:

Afrontar un proceso formal de auditoría como sujeto responsable por parte de la Organización y las prácticas adecuadas en su gestión.

Que el alumno pueda comprender y responder los informes de auditoría tomando las acciones correctivas y oportunidades de mejora solicitadas por los auditores.

Auditoria Informática y Seguridad.

Conceptos de Control Interno y Auditoría.
Metodología de Auditoría Informática. Plan de auditoría.
Segregación de funciones en áreas de IT: Control por oposición, incompatibilidades.
Auditoria de la administración de la Seguridad.
Informes de Auditoría – Evidencia – Irregularidades – Documentación – Informes de auditoría.

Presupuesto horario teoría: 12 horas

<u>Temas de práctica en laboratorio:</u>

Conceptos comunes a todos los Sistemas Operativos
Agrupaciones de Almacenamiento / Trabajos Activos / Estados de Trabajos en Espera (Corta, Corta Ampliada, Larga e Inelegible) / Control de Actividad / Administración de Base de Datos

Presupuesto horario práctica: 8 horas

Presupuesto horario total: 20 horas

Bibliografía[8]

Obligatoria o básica:

Título	Autor/es	Editorial	Año de Edición
Auditoria de Seguridad Informática	Chicano Tejada Ester	IC Editorial	2014
Redes de Computadoras	Andrew S. Tanenbaum / David J. Wetherall	Pearson	2012
Auditoria Informática – Un enfoque Practico	Mario Piattini	AlfaOmega-Ra Ma	2004
Planes de Contingencia	Juan Gaspar Martinez		2004

Complementaria:

Título	Autor/es	Editorial	Año de Edición
Cobit 5 – IT Governance Instituto	IT Governance Instituto	ISACA	2012

[8] *Para textos: citar autor, título, ciudad, editorial, año. Para revistas: citar autor, título del artículo, nombre de la revista, n°, lugar, edición, año, páginas., Para sitios web: dirección de la página.*

Propuesta Pedagógica

Contenido propuesto:

El papel de los alumnos será activo a través de la interacción con el docente y la resolución de ejercicios prácticos sobre sistemas informáticos de rango superiores, los conceptos teóricos serán proporcionados por el docente apoyados por la bibliografía de la cátedra y publicaciones técnicas; progresivamente se irán organizando las clases prácticas con resoluciones individuales. De esta manera, los contenidos teóricos serán consolidados a través de prácticas de resolución individual con asistencia y tutoría del docente.
El cursado brindará los conocimientos relacionados con la administración y gestión de Riesgos y los conceptos básicos de gerenciamiento de gestión de la seguridad y abordaje de auditorías externas.
Las clases serán expositivas con apoyo de trabajos prácticos sobre las diferentes unidades los cuales se desarrollaran con la supervisión y apoyo del docente. Las clases, material de estudio y herramientas pedagógicas tendrán el soporte del CVG, campus virtual de la Facultad Regional Rosario.
Además de un parcial que se realizará luego del cursado del 70% de los contenidos, los alumnos realizarán un trabajo práctico final donde abórde un caso de estudio poniendo en práctica los principales temas estudiados durante el cursado.

Demandas educativas.

La evolución de las tecnologías de la información descentralizadas y el crecimiento en escala de las mismas como así también la utilización de plataformas y software como servicios sumado al creciente control exigido por los organizamos de control en los que considera a la tecnología como uno de los activos más importantes de la Organización hace que los profesionales de Sistemas tengan que tener un conocimiento de las diferentes aspectos de gestión y administración de las mismas.

Elementos a utilizar en el dictado de la asignatura:

- Clases expositivas.
- CVG - Campus Virtual de la Facultad Regional Rosario.
- Resolución de casos problemas.
- Utilización de recursos de multimedia
- Páginas WEB de apoyo.
- Utilización de Bibliografía obligatoria Aportes de apuntes por parte del profesor.

Evaluación

- Examen Parcial
- Presentación de trabajo sobre seguridad y auditoria.

Asignaturas Correlativas del plan[9]

Asignaturas regulares para el cursado:	Redes de Información y Administración de Recursos
Asignaturas aprobadas para el cursado:	Comunicaciones
Asignaturas aprobadas para rendir:	

[9] *No está permitido indicar asignaturas electivas como correlativas. Además todos los cuadros deben estar completados.*

Justificación de correlatividades

Tanto el diseño de base de datos relacionales, el desarrollo de aplicaciones en el cursado de práctica y gestión de las mismas, como así también la inserción del área de Tecnología de la Información en la Organización justifica las asignaturas regulares para su cursado. El mismo criterio aplica para las asignaturas que son necesarias para poder rendir.

Asignaturas Equivalentes respecto del plan anterior[10]

Asignatura/s equivalente respecto del plan anterior:	

[10] *Consignar asignaturas que se pueden otorgar como equivalentes para las posibles solicitudes de cambio de plan.*