Ministerio de Capital Humano
Universidad Tecnológica Nacional
Facultad Regional Rosario

Rosario, 17 de diciembre de 2024.-

VISTO el Expediente ID Nº 8168436, relacionado con la presentación del Programa Analítico de la asignatura "Seguridad en los Sistemas de Información", correspondiente a la carrera Ingeniería en Sistemas de Información – Plan 2023, y

CONSIDERANDO

Que la presentación realizada obedece a la implementación del nuevo Diseño Curricular aprobado por el Consejo Superior de la Universidad Tecnológica Nacional – Ordenanza N° 1877.

Que dicho Programa Analítico cuenta con el aval del respectivo Consejo Departamental.

Que la Comisión de Enseñanza analizó el Expediente y aconsejó su aprobación.

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

EL CONSEJO DIRECTIVO DE LA FACULTAD REGIONAL ROSARIO
DE LA UNIVERSIDAD TECNOLÓGICA NACIONAL
R E S U E L V E:

ARTÍCULO 1º.- Aprobar el Programa Analítico de la asignatura "Seguridad en los Sistemas de Información" para el quinto nivel de la carrera Ingeniería en Sistemas de Información – Plan 2023, que se agrega como Anexo I de la presente resolución.

ARTÍCULO 2º.- Regístrese. Comuníquese. Cumplido, archívese.

RESOLUCIÓN Nº **832**

UTN FRRo
C.D.
S.R.

Ing. Rubén Fernando CICCARELLI
Decano

Ing. Antonio Luis MUIÑOS
Secretario Académico

Carrera: Ingeniería en Sistemas de Información

Asignatura: Seguridad en los Sistemas de Información

PROGRAMA ANALÍTICO

1. Datos administrativos de la asignatura

Nivel en la carrera:	5	Dictado:	Cuatrimestral
Plan de Estudio:	2023	Área:	Gestión Ingenieril
Bloque curricular:	Tecnologías Aplicadas	Electiva:	NO
Carga horaria presencial semanal (hs. cátedra):	6	Carga Horaria total anual (hs. reloj):	72
Carga horaria no presencial semanal (hs. reloj) (si correspondiese)	0	% horas no presenciales (hs. reloj) (si correspondiese)	0

2. Presentación, Fundamentación

El programa de la asignatura ***Seguridad en los Sistemas de Información*** *se concibe dentro de un contexto de actividades reservadas y competencias específicas del diseño curricular de la carrera Ingeniería en Sistemas de Información además de articular y complementar conocimientos adquiridos en las cátedras de la carrera. 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 eventos de seguridad y principalmente la gestión de la seguridad como políticas de las Organizaciones junto al cumplimiento de normativas y regulaciones sustentan los objetivos de la asignatura.
La asignatura contribuye al desarrollo de las competencias especificas (CE 1.1, 2.1, 3.1, 4.1, 5.1 y 7.1) del diseño curricular de la carrera.

3. Contenidos Mínimos

- Seguridad de la Información.
- Marco Normativo.
- Gestión de Riesgos.
- Sistemas de gestión de seguridad.
- Auditoría de Sistemas de Información.
- Peritaje informático forense.

4. Objetivos establecidos en el DC

- **Aplicar modelos de referencia en la gestión de la seguridad de la información según las normativas vigentes.**
- **Planificar controles de seguridad basados en la gestión de riesgo.**
- **Desarrollar un plan de seguridad asegurando la continuidad del negocio.**
- **Comprender el proceso de auditoría y tratamiento de evidencias.**

5. Asignaturas correlativas previas

Para cursar y rendir debe tener cursada:

- Asignatura/s:
  Redes de datos
  Administración de Sistemas de Información

Para cursar y rendir debe tener aprobada:

- Asignatura/s:
  Desarrollo de Software
  Comunicación de datos

6. Asignaturas correlativas posteriores

Indicar las asignaturas correlativas posteriores:

- Asignatura/s que la requieren cursada:
  -
- Asignatura/s que la requieren aprobada:
  -

7. Programa analítico

Este programa analítico contempla los contenidos mínimos, previstos en el DC vigente, y aquellos que se consideran necesarios para desarrollar los resultados de aprendizaje propuestos.

Unidad Nº: 1

Título: **Seguridad de la Información**

Contenidos:

1. **Introducción a la seguridad de los Sistemas de Información.**
2. **Marco Normativo de Gestión de la Seguridad en los Sistemas de información.**[1]

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

Sistemas de Gestión de la Seguridad de la Información

Introducción a Sistemas de Gestión de Seguridad de la Información: Políticas de seguridad, Evaluación, administración y Gestion 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.

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

Unidad Nº: **2**

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

Título: **Seguridad aplicada**

Contenidos:

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

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.

Unidad Nº: 3

Título: **Criptografía y Hacking Ético.**

Contenidos:

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

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

Unidad Nº: 4

Título: **Auditoria Informática y Seguridad.**

Contenidos:

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

Auditoria Informática y Seguridad

Conceptos de Control Interno y Auditoría.

Metodología de Auditoría Informática. Plan de auditoría.

Peritaje Informático Forense.

Segregación de funciones en áreas de IT: Control por oposición, incompatibilidades.

Auditoría de la administración de la Seguridad.

Informes de Auditoría – Evidencia – Irregularidades – Documentación – Informes de auditoría.

Carga horaria por tipo de formación práctica de toda la asignatura

Tipo de formación práctica	Horas reloj
Formación experimental	16
Análisis y resolución de problemas de ingeniería y estudios de casos	32

Formulación, análisis y desarrollo de proyectos.	16

Bibliografía Obligatoria:

William Stalling, 2004, Comunicaciones y Redes de Computadoras, Prentice Hall

Edgar Vega Briceño, 2021, Seguridad de La Información, 3Ciencias

Juan Gaspar Martinez, 2008, Planes de Contingencias y de la Continuidad del Negocio,2008, Diaz de Los Santos..

Bibliografía optativa y otros materiales a utilizar en la asignatura:

ISO-IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls

IRAM-ISO-IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Asignatura equivalente respecto al Plan Anterior

Seguridad en los Sistemas de Información – Plan 2008