Ministerio de Educación
Universidad Tecnológica Nacional
Facultad Regional San Francisco

2022 - Las Malvinas son argentinas

San Francisco, 21 de diciembre de 2022

VISTO la Resolución de Consejo Directivo Nº 481/2022, la Ordenanza N° 1549 y el proceso de acreditación de carreras de grado solicitado por CONEAU, y

CONSIDERANDO:

Que la Resolución de Consejo Directivo Nº 481/2022 aprueba el nuevo modelo de planificación que incluye el programa analítico utilizado por la Facultad Regional San Francisco.

Que la Ordenanza 1549 Reglamento de Estudio para todas las carreras de grado de la UTN, en su artículo 8.2.1 establece "El programa sobre el cual versará la instancia de evaluación final será el programa analítico completo de la asignatura, aprobado por el Consejo Directivo y vigente al momento de rendir."

Que el sistema de CONEAU Global solicita como anexo en la sección de las materias curriculares de cada carrera, la carga del programa analítico, desprendido de la planificación de la asignatura.

Que la Comisión de Enseñanza del Consejo Directivo de la Facultad Regional San Francisco, ha analizado la propuesta y avala la solicitud.

Que el dictado de la medida se efectúa en uso de las atribuciones otorgadas por el Estatuto Universitario.

Por ello,

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

ARTÍCULO 1°.- Aprobar el Programa Analítico de la asignatura Seguridad en los Sistemas de Información, de la carrera Ingeniería en Seguridad en los Sistemas de Información, Plan 2023, Ordenanza Nº 1877 del Diseño Curricular, 5º nivel, cuya carga horaria anual es de 3 hs. y con régimen de dictado cuatrimestral, según ANEXO I que se adjunta a la presente.
ARTÍCULO 2°.- Regístrese, comuníquese, cumplido archívese.

RESOLUCIÓN CD N°: 687/2022

Ing. JUAN C. CALLONI
Secretario
Académico

Ing. Alberto R. TOLOZA
Decano

UNIVERSIDAD TECNOLOGICA NACIONAL

FACULTAD REGIONAL SAN FRANCISCO

Carrera/as:

Ingeniería en Sistemas de Información

Asignatura

Seguridad en los Sistemas de Información

PROGRAMA ANALÍTICO

PLAN 2023

Contenido

1. DATOS ADMINISTRATIVOS DE LA ASIGNATURA

Departamento:	Ingeniería en Sistemas de Información.
Carrera/as:	Ingeniería en Sistemas de Información.
Asignatura:	Seguridad en los Sistemas de Información
Nivel de la carrera	Quinto Nivel
Duración hs cátedras	96 horas cátedras
Bloque curricular:	Tecnologías Aplicadas
Régimen:	Segundo Cuatrimestre - Cuatrimestral
Área:	Gestión Ingenieril

2. PROGRAMA ANALÍTICO EJE/UNIDAD

Explicitar el Programa analítico de la asignatura detallando: Unidades/ Ejes temáticos/ Contenidos / Carga horaria por unidad - Carga horaria por tipo de formación práctica (si correspondiese). Debe incluir los **Contenidos Mínimos** previstos en el Diseño Curricular Vigente. Explicar el programa detallando: Unidades/ Ejes temáticos/ Contenidos /carga horaria por Unidad y por tipo de formación práctica.

Contenidos mínimos según Ord 1877
- Seguridad de la Información. - Marco Normativo. - Gestión de Riesgos. - Sistemas de gestión de seguridad. - Auditoría de Sistemas de Información. - Peritaje informático forense.

PROGRAMA ANALÍTICO

Unidad 1: Introducción a la Seguridad de la Información

1. Conceptos básicos de seguridad de la información.
2. Importancia y objetivos de la seguridad de la información.
3. Principios de la seguridad de la información.
4. Seguridad de la Información y Protección de Datos. Propiedades de confidencialidad, integridad, disponibilidad y autenticidad de la Información. Riesgo: concepto y componentes.
5. Valoración e impacto del riesgo en las organizaciones. Gestión del riesgo. Sistema de Gestión de Seguridad de la Información.
6. Amenazas y vulnerabilidades comunes. Ataques Informáticos. Amenazas. Ingeniería Social. Diferentes tipos de ataques informáticos. Medios de transmisión de amenazas. Técnicas para asegurar la información.
7. Políticas de Seguridad. Grado de madurez de las instituciones. Seguridad física y lógica de los distintos componentes de la arquitectura informática. Protocolos de seguridad informática.
8. Cultura de la seguridad de la información. Relación de la Seguridad Informática con la Informática Forense.

Unidad 2: La Ciberdefensa.

1. La Ciberdefensa, marco teórico (Evolución de los conceptos, definiciones de Ciberdefensa, Ciberseguridad y Ciberespacio).
2. Diferencias entre Ciberdefensa y Ciberseguridad
3. Infraestructura Crítica
4. Operaciones de Ciberdefensa
5. EL Derecho Internacional y la Ciberdefensa
6. La guerra cibernética y la diferencia con otros tipos de ataques.
7. El Derecho Internacional Público
8. Diferencia con la normativa del Derecho Informático local.

Unidad 3: Seguridad y defensa cibernética

1. Arquitectura de los Sistemas. Control de Accesos.
2. Desarrollo de aplicaciones seguras.
3. Seguridad física.
4. Dispositivos y características de las redes de datos.
5. Continuidad de las operaciones.
6. Ciclo de vida de respuesta a un incidente
7. Categorización a los incidentes de seguridad.
8. Guía para el manejo de incidentes.
9. Guía para el manejo del incidente "acceso no autorizado (ANA)".
10. Guía para el manejo de incidente "denegación de servicios (DDS)".
11. Guía para el manejo de incidente "código malicioso (CML)".
12. Procedimientos para el manejo de un ciberincidente

Unidad 4: Marco Normativo

1. Normativas y estándares internacionales en seguridad de la información (ISO/IEC 27001, NIST, GDPR, etc.).
2. Requisitos legales y regulatorios para la protección de datos.
3. Análisis comparativo de normativas y estándares.
4. Implementación de marcos normativos en organizaciones.

Unidad 5: Gestión de Riesgos

1. Concepto de riesgo en seguridad de la información.
2. Identificación y evaluación de riesgos.
3. Análisis cuantitativo y cualitativo de riesgos.
4. Métodos y técnicas para la gestión de riesgos.
5. Planificación y desarrollo de estrategias de mitigación de riesgos.

Unidad 6: Sistemas de Gestión de Seguridad de la Información (SGSI)

1. Diseño e implementación de un SGSI.
2. Procesos de un SGSI según ISO/IEC 27001.
3. Políticas, procedimientos y controles de seguridad.
4. Documentación y registro de actividades en un SGSI.
5. Auditorías internas y externas de un SGSI.

Unidad 7: Auditoría de Sistemas de Información

1. Concepto y objetivos de la auditoría de sistemas.
2. Planificación y ejecución de auditorías de seguridad.
3. Herramientas y técnicas de auditoría.
4. Identificación y manejo de hallazgos de auditoría.
5. Informes de auditoría y seguimiento de recomendaciones.

Unidad 8: Peritaje Informático Forense

1. Introducción al peritaje informático forense.
2. Procedimientos y metodologías en peritaje informático.
3. PURI Proceso unificados de recolección de Información
4. Recopilación y preservación de evidencia digital.
5. Análisis de incidentes de seguridad.
6. Elaboración de informes periciales y presentación de testimonios.

Unidad 9: Actuación Forense

1. Introducción a la Criminalística. Criminalística. Principios de la Criminalística. Ciencias Forenses. Principios Forenses.
2. Metodología de la investigación en el lugar del hecho. El reconocimiento de la escena. La inspección ocular. Observación. Documentación: Descripción. Fotografías forenses. Escalas.
3. Los delitos informáticos. Regulación europea y argentina. El Convenio de Cibercriminalidad de Budapest. La regulación de los Delitos Informáticos en Argentina. Delito transnacional. Jurisdicción y competencia.
4. La Investigación. La actividad investigativa en el contexto del proceso penal. Investigación, prueba y argumentación judicial.
5. Finalidades de la investigación penal.
6. La denuncia. La Investigación Criminal. La informática forense en el lugar del hecho.
7. Recolección de la evidencia. Cadena de Custodia. Protocolo de Actuación en Informática Forense.
8. Actuación Forense y Guía Integral de empleo de la Informática Forense en el Proceso penal.
9. Prueba. El valor y validez de la prueba. La prueba. La pericia. El perito.
10. Perito de parte y de oficio. Perito oficial. Diferencias. Deberes y obligaciones. Perito Informático. Leyes de ejercicio profesional. Responsabilidad y ética profesional.

11. Prueba Científica. Prueba Informática. Conceptos generales sobre Protocolos y Guías de buenas prácticas.
12. Técnicas de Comunicación. El abordaje interdisciplinario. El lenguaje claro. La traducción de lenguaje técnico en lenguaje coloquial. La argumentación científica.