San Francisco, 4 de abril de 2024

VISTO lo dispuesto por la Ordenanza 1383/12 y la propuesta del Departamento de Ingeniería en Sistemas de Información, y

CONSIDERANDO:

Que por medio de esta normativa y mediante el dictado de asignaturas electivas es posible incorporar perfiles propios de la región a efectos de adaptar los diseños curriculares a las necesidades de la misma.

Que en tal sentido y en cumplimiento de las reglamentaciones vigentes, y a propuesta de los Departamentos respectivos los Consejos Directivos de las Facultades Regionales definirán cuáles serán las materias electivas, área del conocimiento, objetivos generales y específicos que justifiquen la inclusión, carga horaria, sus contenidos analíticos, bibliografía, modalidad de dictado, propuesta pedagógica, y sus correspondientes correlatividades debidamente justificadas.

Que el Consejo Departamental de Ing. en Sistemas de Información elevó al Consejo Directivo de esta Facultad Regional San Francisco la propuesta de implementación de materias electivas.

Que la Comisión de Enseñanza del Consejo Directivo de la Facultad Regional San Francisco, ha analizado los antecedentes 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 dictado de la asignatura Seguridad en los Sistemas de Información (carga horaria anual 3 hs.) como materia electiva, parte curricular de la Carrera Ingeniería en Sistemas de Información - Plan 2008, del área Gestión Ingenieril a dictarse en el quinto nivel, con modalidad cuatrimestral (2do cuatrimestre) y una carga horaria de 6 hs. semanales, a partir del Ciclo Lectivo 2024.
ARTÍCULO 2°.- Aprobar en Anexo I, Objetivo General y objetivos específicos que justifican la inclusión de dicha materia, las correlatividades debidamente justificadas, el programa analítico, la bibliografía y la propuesta pedagógica.
ARTÍCULO 3°.- Otorgar equivalencia en la asignatura Seguridad en los Sistemas de Información (Materia curricular) - Plan 2023 de la carrera Ingeniería en Sistemas de

Información, sólo para aquellos estudiantes que regularizaron y/o aprobaron la asignatura Seguridad en los Sistemas de Información (Electiva) - Plan 2008.
ARTÍCULO 4°.- Regístrese. Comuníquese. Elévese al Rectorado a sus efectos y archívese.

RESOLUCIÓN CD N°: 377/2024

Ing. JUAN CARLOS CALLONI
Secretaría Académica

Firma Digital

Aprobación del Documento por Juan Carlos Calloni
UNIVERSIDAD TECNOLÓGICA NACIONAL FR SAN FRANCISCO

Ing. Alberto R. TOLOZA
Decano

Firma Digital

Aprobación del Documento por Alberto Toloza
UNIVERSIDAD TECNOLÓGICA NACIONAL - FR SAN FRANCISCO

Ministerio de Capital Humano
Universidad Tecnológica Nacional
Facultad Regional San Francisco

Res CD Nº 377/2024

Anexo I

Seguridad en los Sistemas de Información
(Electiva – Plan 2008)

1. Objetivos generales y específicos que justifican la inclusión de la Materia

Objetivo General:

Adquirir los conocimientos, habilidades y competencias necesarias para enfrentar los desafíos y amenazas en materia de seguridad de la información, y que puedan contribuir eficazmente a la protección de los activos tecnológicos y al cumplimiento de los objetivos organizacionales en un contexto de constante evolución tecnológica y normativa. Aplicando los modelos de referencia conforme a normativas vigentes, la planificación de controles de seguridad basados en la gestión de riesgos, el desarrollo de planes de seguridad que aseguren la continuidad del negocio, y la comprensión del proceso de auditoría y tratamiento de evidencias

Objetivos específicos:

- Introducir a los estudiantes en los modelos de referencia para la gestión de la seguridad de la información, como ISO 27001, NIST Cybersecurity Framework, entre otros, y proporcionarles las habilidades para aplicar estos modelos según las normativas vigentes.
- Aplicar las herramientas necesarias para identificar, evaluar y gestionar los riesgos en los sistemas de información, y planificar controles de seguridad efectivos basados en una evaluación de riesgos completa.
- Diseñar Planes de Seguridad integrales que garanticen la continuidad del negocio ante posibles amenazas y eventos disruptivos, considerando aspectos como la recuperación ante desastres, la gestión de incidentes y la protección de la información crítica.
- Desarrollar Procesos de Auditoría de seguridad, incluyendo la identificación de evidencias, la evaluación de controles y la elaboración de informes para garantizar el cumplimiento de los estándares de seguridad y las regulaciones pertinentes.

Ministerio de Capital Humano
Universidad Tecnológica Nacional
Facultad Regional San Francisco

2. Correlatividades debidamente justificadas

Para Cursar:

Regularizadas

a. **Redes de Información**: Conceptos básicos de redes: protocolos, topologías, modelos de red (OSI y TCP/IP) y dispositivos de red. Seguridad en redes: amenazas y vulnerabilidades específicas de las redes informáticas, protocolos de seguridad (como HTTPS y VPN) y medidas de protección para redes (como firewalls y sistemas de detección de intrusiones).
b. **Administración de Recursos**: Esta materia es necesaria tenerla cursada por la gestión de riesgos en seguridad informática es un proceso integral que permite a las organizaciones que administran recursos identificar, evaluar, priorizar y tratar los riesgos de seguridad, garantizando la protección de sus activos y la continuidad de sus operaciones.

Aprobadas

a. **Comunicaciones**: Conceptos básicos de redes: topologías, modelos de red (OSI y TCP/IP), dispositivos de red y protocolos de comunicación. Funcionamiento de las redes de datos y su papel en la transmisión de información. Seguridad en las redes: amenazas comunes, vulnerabilidades y medidas de protección.

Para Rendir:

Aprobadas

a. **Redes de Información**: Conceptos básicos de redes: protocolos, topologías, modelos de red (OSI y TCP/IP) y dispositivos de red. Seguridad en redes: amenazas y vulnerabilidades específicas de las redes informáticas, protocolos de seguridad (como HTTPS y VPN) y medidas de protección para redes (como firewalls y sistemas de detección de intrusiones).
b. **Administración de Recursos**: Esta materia es necesaria tenerla cursada por la gestión de riesgos en seguridad informática es un proceso integral que permite a las organizaciones que administran recursos identificar, evaluar, priorizar y tratar los riesgos de seguridad, garantizando la protección de sus activos y la continuidad de sus operaciones.

Ministerio de Capital Humano
Universidad Tecnológica Nacional
Facultad Regional San Francisco

3. 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

Ministerio de Capital Humano
Universidad Tecnológica Nacional
Facultad Regional San Francisco

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.

Ministerio de Capital Humano
Universidad Tecnológica Nacional
Facultad Regional San Francisco

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.

4. Bibliografía

(Bibliográficas y No bibliográficas)

OBLIGATORIA:

- CORLETTI ESTRADA, Alejandro.
  Ciberseguridad: Una Estrategia Informático militar. [archivo electrónico]
  [1a. ed. en español].En Línea
  Madrid, España. DarFe Learning Consulting S.L, 2017.
  ISBN 978-84-697-7205-8.
  (Al 2023: 0 ejemplar/es en colección UTN,
  1 acceso digital multiusuario en plataforma darFe.es Disponible en:
  https://darfe.es/es/descarga-nuestros-libros

- CORLETTI ESTRADA, Alejandro.
  Seguridad en Redes. [archivo electrónico]
  [1a. ed. en español].
  Madrid, España. DarFe Learning Consulting S.L, 2016.
  ISBN 978-84-617-5291-1.
  (Al 2023: 0 ejemplar/es en colección UTN,
  1 acceso digital multiusuario en plataforma darFe.es Disponible en:
  https://darfe.es/es/descarga-nuestros-libros

- DOMINGUEZ CHÁVEZ, Jorge.
  Fundamentos de Auditoría Informática. [archivo electrónico]
  [1a. ed. en español].
  Venezuela. IEASS, Editores, 2021.
  ISBN 9789806366107.
  (Al 2023: 0 ejemplar/es en colección UTN,
  1 acceso digital multiusuario en plataforma Researchgate Disponible en:
  https://www.researchgate.net/publication/349505412_Fundamentos_de_Auditoria_Informatica

- GÓMEZ VIEITES, Álvaro.
  Auditoría de Seguridad Informática. [en línea]
  [1a. ed. en español].
  Madrid, España. RA-MA Editorial, 2015.
  E-ISBN 9788499643281.
  (Al 2023: 0 ejemplar/es en colección UTN,
  1 acceso digital multiusuario en plataforma e-Libro Disponible en:
  https://elibro.net/es/ereader/utnfrsfco/62464?
  [consulta 03/03/2023]

- LOPÉZ, Ricardo Alfredo.
  Sistema de Gestión de la Seguridad Informática. [archivo electrónico]
  [1a. ed. en español].
  Bogotá. Fundación Universitaria del Área Andina, 2017.
  ISBN 978-958-5455-74-0.
  (Al 2023: 0 ejemplar/es en colección UTN,
  1 acceso digital multiusuario en plataforma RIA Área Andina Disponible en:
  https://digitk.areandina.edu.co/handle/areandina/1238?show=full&locale-attribute=en

- PÉREZ, Julio César.
  Protección de datos y seguridad de la información: guía práctica para ciudadanos y empresas. [en línea]
  (4a. ed. En español).
  Madrid, España. RA-MA Editorial, 2015.
  E-ISBN 9788499645919.
  (Al 2023: 0 ejemplar/es en colección UTN,
  1 acceso digital multiusuario en plataforma e-libro Disponible en:
  https://elibro.net/es/ereader/utnfrsfco/106483?page=5.
  [consulta 03/03/2023]

COMPLEMENTARIA:

- AZAHUANCHE GUTIÉRREZ, Sergio.
  Auditoría de Tecnologías con un enfoque de hacker ético. [archivo electrónico]
  [1a. ed. en español].
  Bolivia. CLAIN, 2019.
  ISBN 978-84-697-7205-8.
  (Al 2023: 0 ejemplar/es en colección UTN,
  1 acceso digital multiusuario en plataforma felban Disponible en:
  https://felaban.s3-us-west-2.amazonaws.com/memorias/archivo20190605142700PM.pdf

- SANTACRUZ ESPINOZA, Julio Jhovany; VEGA ABAd, Cesar Remigio; PINOS CASTILLO, Luis Fernando; CÁRDENAS VILLAVICENCIO, Oscar Efren.
  Sistema COBIT en los procesos de auditorías de los sistemas Informáticos. [archivo electrónico]
  En: Journal Of Science And Research: Revista Ciencia E Investigacion, 2017.
  E-ISSN: 2528-8083, VOL. 2, NO. 8, Octubre - Diciembre 2017, PP. 65-68.
  (Al 2023: 0 ejemplar/es en colección UTN,
  1 acceso digital multiusuario en plataforma Dialnet Disponible en:
  https://dialnet.unirioja.es/servlet/articulo?codigo=7344282

Ministerio de Capital Humano
Universidad Tecnológica Nacional
Facultad Regional San Francisco

5. Propuesta pedagógica

Estrategias didácticas

- Interrogatorio dialogado.
- Trabajos en pequeños grupos:
- Debates.
- Resolución de problemas y casos.
- Ejemplificaciones.
- Actividades en TP integrador para la expresión oral.

Recursos metodológicos

- La lluvia de ideas.
- La elaboración de estrategias de resolución de problemas y casos.
- La planificación conjunta del aprendizaje.
- El método de casos.

Secuencia Metodológica

- Clase Discusión sobre la planificación.
- Clases expositiva dialogada con la PC, el cañón y el pizarrón o pizarra electrónica.
- Trabajos en grupo para la conclusión final.
- Trabajos prácticos y Casos en Laboratorio.
- Talleres en el laboratorio.
- Trabajo práctico Integrador en una empresa sobre un caso real.
- Visitas a la Municipalidad viendo un caso real de una red.
- Talleres en el laboratorio con utilización de PC o bien en máquinas virtuales preparadas para tal fin.
- Exposición de cada grupo del trabajo integrador.

Recomendaciones para estudiantes

Partiendo de la base que los estudiantes deben conocer y haber asimilado los sistemas de transmisión de datos y de comunicación entre maquinas computacionales, el manejo de la notación binaria y los términos propios de los ambientes computacionales. Poseer conocimientos previos de la arquitectura de los distintos SOR. Además deberán

- Tomar Apuntes de lo que se expone en clases.
- Repasar lo que se ha avanzado semana tras semana
- Organiza tu calendario para anticiparte a las fechas de evaluación
- Trata de no leer tanto tiempo seguido de pantallas toma descansos.
- Mantén apagadas o en silencio las redes sociales en clase y cuando estudies para que no te distraigan
- Asiste a clases
- No dejes todo para él último

- Consulta las dudas a los profesores
- Cada TP o Caso no tiene una única solución.
- No estudies la teoría para recitarla, trata de entender para que utiliza, y como nos ayuda a resolver los problemas y casos planteados por la materia.