Programa de
INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA
(Tecnólogo en Informática)

1. NOMBRE DE LA UNIDAD CURRICULAR

Introducción a la seguridad informática

2. CRÉDITOS

8 créditos

3. OBJETIVOS DE LA UNIDAD CURRICULAR

- Adquirir los conceptos fundamentales de la ciberseguridad, reconociendo las características principales de esta disciplina.
- Analizar el Marco Legal y Regulatorio (Uruguay e Internacional) para generar conciencia profesional y ética.
- Disponer de un conocimiento inicial de once Dominios de Seguridad y aplicar principios para la construcción de defensas técnicas y arquitectónicas.
- Introducir al estudiantes en los conceptos básicos de ingeniería social.
- Experimentar y comunicar métodos y herramientas de seguridad avanzada a través de demostraciones prácticas.
- Evaluar la Postura de Riesgo de una organización, elaborando un Inventario de Activos, un Modelo de Amenazas y un Plan de Gestión de Riesgos.

4. METODOLOGÍA DE ENSEÑANZA

Componente	Horas de Clase (Semanales)	Horas Totales (15 Semanas)
Teórico (T)	2 hora	30 horas
Práctico / Laboratorio Asistido (P/L)	2 horas	30 horas
Dedicación No Presencial (Personal)	4 horas (estimado)	60 horas (estimado)
Total Estimado	8 horas	120 horas

Participación de los Estudiantes:

- Demostraciones Prácticas: El instructor realizará demostraciones en el laboratorio de herramientas (Nmap, Netcat, ZAP), ingeniería social y técnicas de

ataque/defensa durante las horas de clase, para ilustrar los conceptos del dominio semanal.

- Presentaciones Grupales (Parcial 1): Los estudiantes realizarán presentaciones de 25 minutos en grupos, demostrando habilidades prácticas de investigación en seguridad.
- Proyecto de Riesgos (Evaluación Final): Realización de un proyecto de modelado y gestión de riesgos para una empresa ficticia.

5. TEMARIO

Tema	Descripción y subtemas
TEMA I: Introducción, fundamentos y marco legal	Introducción, Aspectos Legales, Reglamentarios y Cumplimiento. Introducción, Motivación, la Tríada CIA. Marco Legal Uruguayo: Ley N.º 18.331 y Delitos Informáticos. Marcos Internacionales (GDPR, OWASP).
TEMA II: Herramientas Criptográficas y Seguridad de Activos	Dominio: Seguridad de los Activos. Criptografía: Hashing, Simétrico/Asimétrico. Integridad de Datos.
TEMA III: IAM y Arquitectura de Red	Dominio: IAM y Arquitectura de Red. Control de Acceso (RBAC). Protocolos de Red. Herramientas: Nmap y John the Ripper.
TEMA IV: Seguridad en Desarrollo, Operaciones, Ingeniería Social	Dominios: AppSec, OpSec y Evaluación. Vulnerabilidades de Aplicaciones: XSS, SQLi (Remediación). Ingeniería Social y Detección. Netcat y ZAP.
TEMA V: Gestión de Riesgos y Continuidad	Dominios: Seguridad y Gestión de Riesgos, BCDR. Modelado de Amenazas, Inventario de Activos, Planificación de la Continuidad del Negocio.

6. BIBLIOGRAFÍA

Tema	Básica	Complementaria
TEMA I a V	(1)	(2), (3), (5)
TEMA I, IV, V		(4)

6.1 Básica

1. Stallings, W., Brown, L. (2018). Computer Security: Principles and Practice, 4th Edition. Pearson.

6.2 Complementaria

2. Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), AGESIC. Materiales Didácticos de la campaña “Seguro te conectás”. Disponible en: https://www. gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/ciudadania.
3. (ISC)². (Versión Reciente). CISSP Official Study Guide. (Referencia para la estructura y conceptos de Dominios de Seguridad).
4. Tevault. Mastering Linux Security and Hardening: Protect your Linux systems from intruders, malware attacks, and other cyber threats , Second Edition. Packt.
5. OWASP Foundation. (Última versión). OWASP Top 10 y OWASP API Security Top 10.

7. CONOCIMIENTOS PREVIOS EXIGIDOS Y RECOMENDADOS

7.1 Conocimientos Previos Exigidos: Se requieren conocimientos de Administración de Infraestructura, Programación Avanzada y Bases de Datos.

7.2 Conocimientos Previos Recomendados: Conocimiento básico de los protocolos TCP/IP, conocimientos básicos de sistemas operativos, programación y base de datos

ANEXO A
Para todas las Carreras

A1) INSTITUTO

Comisión Nacional de Carrera del Tecnólogo en Informática (UTU-UTEC-UDELAR)

A2) CRONOGRAMA TENTATIVO

Semana	Temas y Dominios (4 hs de clase)	Foco Práctico (2 hs)
Semana 1	TEMA I: Introducción ala seguridad informática, CIA, Riesgo. Marco Legal Uruguayo.	Demostración: Ética y Delito Informático.
Semana 2	TEMA II (Activos/Criptografía). Hashing, Simétrico/Asimétrico. Marcos Internacionales.	Demostración: Integridad de Archivos.
Semana 3	TEMA III Consola Bash. Nmap (Reconocimiento). Presentación Actividad 1.	Demostración: Nmap y uso de Comandos Linux.
Semana 4	TEMA IV (Ingeniería Social). Vectores de ataque, Phishing, tipos de phishing, google dorks, maltego, shodan. Concientización.	Demostración: Análisis de Phishing.
Semana 5	TEMA III (IAM). Autenticación, MFA. John the Ripper (Auditoría de Hashes), Diccionario,Reglas, Fuerza Bruta, Rainbow tables.	Demostración: Auditoría de Contraseñas, fuerza bruta, reconocimiento pasivo.
Semana 6	TEMA IV (AppSec). Introducción a la programación segura con Html, Css y javascript. XSS/SQLi y Principios de Remediación.	Demostración: Fallos de Inyección en Código.
Semana 7	TEMA IV (Herramientas). Netcat y ZAP (Auditoría Web).	Demostración: Netcat y ZAP.
Semana 8	EVALUACIÓN Actividad 1: Presentaciones Grupales (4 hs de clase).	
Semana 9	TEMA V (Monitoreo). tcpdump (Análisis de Tráfico), Análisis de Logs, IDS/IPS.	Demostración: Análisis de Tráfico Anómalo.
Semana 10	TEMA IV (Operaciones). Hardening de SO. Vulnerabilidades Comunes.	Demostración: Auditoría de Permisos.

Semana 11	TEMA V: Modelado de Amenazas (Inicio Proyecto Final).	Práctica: Valoración de Activos, modelar amenazas usando Threat Modeling Tool
Semana 12	TEMA V: Gestión de Riesgos. Metodologías de Análisis y Tratamiento.	Práctica: Desarrollo de la Matriz de Riesgos.
Semana 13	TEMA V: BCDR y Planificación de Continuidad.	Tutoría Proyecto Final.
Semana 14	Revisión General. Revisión de Conceptos Clave de Gestión de Riesgos.	Tutoría Proyecto Final.
Semana 15	EVALUACIÓN FINAL (Parcial 2): Defensa del Plan de Gestión de Riesgos y Modelado de Amenazas (4 hs de clase).	

A3) MODALIDAD DEL CURSO Y PROCEDIMIENTO DE EVALUACIÓN

Instancia de Evaluación	Peso Relativo	Criterio de Aprobación / Descripción
Parcial 1 (Semana 8)	40%	Presentación Oral Grupal (25 min): La evaluación se centra en la investigación, el dominio técnico y la comunicación. La demostración práctica en vivo es obligatoria para la presentación.
Evaluación Final (Parcial 2) (Semana 15)	40%	Defensa del Proyecto de Gestión de Riesgos: El grupo debe entregar y defender oralmente un Inventario de Activos, el Modelo de Amenazas y el Plan de Gestión de Riesgos detallado para un escenario ficticio.
Participación y Asistencia	20%	Evaluación de la participación activa y asistencia.

Aprobación del Curso: Obtener un promedio ponderado mínimo de 60% en el total de las instancias de evaluación. La presentación grupal es obligatoria para aprobar el curso.

A4) CALIDAD DE LIBRE

Esta unidad curricular no adhiere a la resolución del consejo sobre la condición de libre.

A5) CUPOS DE LA UNIDAD CURRICULAR

Cupos mínimos: no tiene
Cupos máximos: no tiene