2

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

Dirección General de Educación Técnico Profesional-UTU
Dirección Técnica de Gestión Académica
Departamento de Diseño y Desarrollo Curricular

PLAN DE ESTUDIO

Identificación	Código SIPE	Descripción		
Tipo de Curso	028	Tecnólogo		
Plan	2023			
Orientación	88F	Ciberseguridad		
Modalidad	Presencial			
Requisitos de Ingreso	Egresados de la Educación Media Superior en sus diferentes modalidades			
Duración		Horas totales:	Horas semanales:	Semanas:
	Técnico	1680	21 y 33	16
	Tecnólogo	2496		
Perfil de Egreso	Competencias Tecnólogo en Ciberseguridad - Aplica las metodologías, tecnologías y herramientas que provee la disciplina en sus entornos profesionales para la implementación y el mantenimiento de políticas y controles de aseguramiento de infraestructuras y sistemas informáticos. - Reconoce los fundamentos de la seguridad de la información, de forma de poder dar apoyo en la aplicación de normativas y estándares, en la gestión de incidentes y riesgos de seguridad y en garantizar la continuidad del negocio, protegiendo los activos críticos. - Integra conocimiento de los procesos de producción vinculados a su área profesional en Uruguay, en sus dimensiones técnica, económica y social, para enfrentarse creativamente a las problemáticas que se le planteen, y tener capacidad de búsqueda y procesamiento de información relevante a su trabajo y de seguir los avances técnicos y metodológicos de las distintas especialidades de la disciplina.			
Certificación	Créditos Educativos	Técnico Superior en Ciberseguridad 164 Tecnólogo en Ciberseguridad 244		
	Título	Técnico Superior en Ciberseguridad Tecnólogo en Ciberseguridad		
Fecha de presentación: 6/3/2023	Exp. N°	Res. N°	Acta N°	Fecha

ANTECEDENTES:

La presente propuesta formativa toma como fundamentos para su construcción los aportes del Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Uruguay[1].

Como se establece en el documento citado "La ciberseguridad como disciplina, esta es una disciplina basada en las tecnologías de la información y la comunicación (TIC), que involucra tecnología, personas, información y procesos, en la que se trata de garantizar que los sistemas informáticos funcionen correctamente en presencia de adversarios. Tiene una fuerte componente interdisciplinar, que incorpora aspectos de gestión de riesgos, derecho, psicología y ética, entre otros".

La formación en las áreas informáticas en la DGETP en nivel Terciario tiene como antecedente la propuesta de la carrera de Tecnólogo en Informática Plan 2007, esta constituye una oferta educativa, la que es ofrecida conjuntamente por la Universidad de la República y la Administración Nacional de Educación Pública (ANEP). Como se menciona en dicho Plan esta formación "busca desarrollar las capacidades para actuar en la realización, puesta en marcha, mantenimiento y administración de sistemas informáticos". Le permitirá a un Tecnólogo en Informática participar como técnico calificado en tareas de desarrollo de proyectos, integrándose al trabajo en equipo para la realización de estas actividades en situaciones de variada complejidad, tanto por sus características como por su escala.

FUNDAMENTACIÓN

En el proceso de transformación educativa en el que se enmarca la ANEP, es de interés para la DGETP impulsar la formación en áreas de innovación a fin de contribuir como misión la mejora sustentable de la matriz productiva, aportando a tales efectos con procesos de formación tecnológica de calidad y con propuestas educativas actualizadas, atendiendo las demandas de desarrollo.

La necesidad formativa se desprende también del avance tecnológico y cibernético del que es característico de esta era. De ello deviene la orientación a la protección de sistemas, redes y programas de los ataques online y las ciberamenazas, a la vez que defiende a la ciudadanía en clave de su ejercicio digital, en el cuidado de datos y sistemas informáticos que protege su identidad y privacidad.

[1] Plan de Estudios de la Carrera Analista Técnico en Ciberseguridad Propuesta de plan curricular e implementación. Equipo integrado por Gustavo Betarte, Juan Diego Campo y Carlos Luna; Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Uruguay. Diciembre 2022.

Es de interés en este marco, presentar una propuesta educativa que posibilite el desarrollo de competencias profesionales que atienden "la aplicación de las metodologías, tecnologías y herramientas que provee la disciplina (como, por ejemplo, la criptografía aplicada, los modelos y mecanismos de autenticación y control de acceso, el desarrollo seguro de aplicaciones, el hardening de sistemas operativos y bases de datos, y la arquitectura de redes seguras) en las áreas en las que la ciberseguridad tiene su aplicación. Debe también estar familiarizado con los fundamentos de la seguridad de la información, de forma de poder dar apoyo en la aplicación de normativas y estándares, en la gestión de incidentes y riesgos de seguridad y en garantizar la continuidad del negocio, protegiendo los activos críticos[2]".

[2] Plan de Estudios de la Carrera Analista Técnico en Ciberseguridad Propuesta de plan curricular e implementación. Equipo integrado por Gustavo Betarte, Juan Diego Campo y Carlos Luna; Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Uruguay. Diciembre 2022. Pág.2.

MALLA CURRICULAR

SEMESTRE	ASIGNATURA	HORA AULA SEMANAL 45'	HORA SEMESTRAL	CRÉDITOS EDUCATIVOS
PRIMER	Introducción a la Programación	8	128	13
	Arquitectura de Computadoras	5	80	8
	Matemática discreta y Lógica 1	4	64	6
	Taller de Introducción a la Seguridad Informática	4	64	6
	Sub Total * 16 SEMANAS	21	336	33
SEGUNDO	Estructura de Datos y Algoritmos	8	128	13
	Sistemas Operativos	5	80	8
	Matemática discreta y Lógica 2	4	64	6
	Introducción a las Bases de Datos	4	64	6
	Inglés Técnico	4	64	6
	Sub Total * 16 SEMANAS	25	400	39
TERCER	Desarrollo seguro de aplicaciones	8	128	13
	Redes de computadoras	5	80	8
	Seguridad de sistemas Operativos	8	128	13
	Criptografía aplicada	8	128	13
	Sub Total * 16 SEMANAS	29	464	47
CUARTO	Taller de programación segura	8	128	13
	Seguridad de Redes de Computadoras	8	128	13
	Taller de Técnicas y Procedimientos	6	96	6
	Gestión de la Seguridad de la Información	8	128	13
	Sub Total * 16 SEMANAS	30	480	45
QUINTO	Pasantía	10	160	16
	Electiva 1	7	112	11

4

	Electiva 2	7	112	11
	Sub Total * 16 SEMANAS	24	384	38
SEXTO	Proyecto Final	13	208	20
	Electiva 3	7	112	11
	Electiva 4	7	112	11
	Sub Total * 16 SEMANAS	27	432	42
	Total semanal		-	-
	CARGA HORARIA TOTAL		2496	-
	Créditos totales de la Carrera	-	-	244

ENFOQUE METODOLÓGICO

Se establecerá un enfoque marcado por la aplicación práctica de los saberes sin ir en detrimento de la fuerte base teórica. La finalidad de la carrera es la aplicación de lo aprendido en las diferentes áreas de implementación y el mantenimiento de políticas y controles de aseguramiento de infraestructuras y sistemas informáticos . Es decir que el cursante luego de aprobar la carrera no encuentre obstáculos formativos o de aplicación en lo que será su futuro desempeño.

La metodología para el desarrollo de la carrera deberá atender necesariamente los aspectos que colaboren a la generación de una mirada analítica de carácter interdisciplinario, que habilite la integración de conocimientos de otros campos del orden científico del campo en que se desarrollará.

En este Plan de estudio, las áreas de conocimientos sobre las que se estructura el cursado a saber: Matemática, Programación, Arquitectura, Sistemas Operativos y Redes de Computadores Bases de datos, Seguridad computacional, Seguridad de la Información y sobre el final de la carrera Actividades Integradoras: talleres, pasantías y proyectos, apuntan fundamentalmente a las cuestiones del método científico y técnico, esencial para el abordaje de nuevos problemas aplicados a la Ciberseguridad.

En busca de mayor potencial de estos profesionales se entiende que una de sus principales aptitudes está dirigida al continuo aprendizaje, la formación, la transmisión y la investigación aplicada en casos y proyectos concretos como ejes primordiales en su preparación.

Se entiende por formación al proceso educativo o de enseñanza y aprendizaje que se vincula a un conjunto de actividades orientadas principalmente a la creación de nuevas habilidades y capacidades en los estudiantes.

Se entiende por investigación al conjunto de actividades orientadas fundamentalmente a la incorporación de conocimientos por parte del estudiante. Así mismo, la formación y la investigación no son instancias separadas dentro del ciclo enseñanza-aprendizaje, una sirve a la otra, y ambas aportan a la creación de buenos profesionales.

De esta manera, el Plan de estudios busca lograr un equilibrio entre el aprendizaje receptivo, definido como el aprendizaje donde el estudiante recibe el contenido que ha de internalizar y el aprendizaje explícito definido como el aprendizaje donde el estudiante es proactivo adaptando los nuevos conceptos a su esquema cognitivo, entendiendo este equilibrio como la complementación de enseñanza-aprendizaje entre lo que el estudiante recibe en aulas formales y lo que el estudiante explora, descubre y relaciona por sí mismo con apoyo docente.

Finalmente, el Plan de estudios se ajusta al marco propuesto y que se adjunta como complemento del presente documento, elaborado por el Instituto de Computación, Facultad de Ingeniería, Universidad de la República, en acuerdo con la Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento (AGESIC). .

EVALUACIÓN

La evaluación se realizará de acuerdo a las pautas establecidas por la DGETP y el reglamento vigente de los cursos terciarios, tanto en lo teórico como en lo práctico atendiendo a la especificidad de la materia.

Todas las materias tienen posibilidad de exoneración, teniendo en cuenta el sistema de previaturas sugerido en la propuesta de plan presentado por AGESIC.

SABERES PREVIOS PARA LA CURSADA DE LAS UNIDADES CURRICULARES		
SABERES RECOMENDADOS PREVIOS	SABERES PREVIOS FUNDAMENTALES	UNIDAD CURRICULAR
Conocimientos previstos en el perfil de ingreso	No tiene	Arquitectura de computadoras
Conocimientos previstos en el perfil de ingreso	No tiene	Programa de Matemática Discreta y Lógica 1
Conocimientos previstos en el perfil de ingreso	No tiene	Introducción a la Programación
Conocimientos previstos en el perfil de ingreso	No tiene	Taller de introducción a la seguridad informática
Conocimientos previstos en el perfil de ingreso	No tiene	Introducción a la Seguridad Informática
Conocimientos previstos en el perfil de ingreso	Matemática Discreta y Lógica 1 (MDL1)	Matemática Discreta y Lógica 2
Conocimientos previstos en el perfil de ingreso	Matemática Discreta y Lógica 1. Introducción a la Programación.	Estructuras de Datos y Algoritmos
Conocimientos previstos en el perfil de ingreso	Matemática Discreta y Lógica 1 y 2. Introducción a la Programación. Estructuras de Datos y Algoritmos.	Programa de Criptografía Aplicada
Desarrollo de aplicaciones, en particular aplicaciones web. Conocimientos generales de metodologías de desarrollo	Estructuras de Datos y Algoritmos.	Desarrollo Seguro de Aplicaciones
Vulnerabilidades comunes en aplicaciones. Conocimientos de desarrollo de aplicaciones	Desarrollo Seguro de Aplicaciones.	Taller de Programación segura
Nociones de física y matemática.	Arquitectura de Sistemas, Sistemas Operativos y Programación.	Redes de Computadoras

No tiene	Estructuras de Datos y Algoritmos. Arquitectura de Sistemas. Sistemas Operativos	Seguridad en Sistemas Operativos
No tiene	Redes de Computadoras	Seguridad en Redes de Computadoras
Definición y aplicación de políticas y procedimientos de Seguridad de la Información y computacional.	Taller de Introducción a la Seguridad Informática.	Taller de Técnicas y Procedimientos
Manejo fluido de conceptos esenciales de arquitectura de computadores y sistemas operativos	Redes de Computadores Seguridad en Redes Seguridad en Sistemas Operativos Seguridad de Aplicaciones	Introducción al Análisis Forense Digital
Criptografía Aplicada, Gestión de la Seguridad de la Información.	Sistemas Operativos Seguridad en Sistemas Operativos Redes de Computadoras, Seguridad en Redes de Computadoras.	Configuración y Administración Segura de Sistemas

HORAS DE COORDINACIÓN

En referencia a la gestión del espació de coordinación se sugiere que la misma se implemente en una sala mensual con 4 horas de duración donde se observen las necesidades de integralidad de los saberes que se abordan en esta especialidad. De esta manera, el espacio dará prioridad a la construcción de actividades integradas que permitan la resolución de problemas, retos y demás metodologías que fortalezcan el componente práctico de la formación.

6

Tecnólogo (028) Ciberseguridad (88F) – Plan 2023		
Perfil de Ingreso	Egresado de Educación Media Superior	
Prueba de suficiencia	No se establece.	
Esquema de Previaturas	**Asignatura previa**	**Asignatura subordinada**
	Matemática Discreta y Lógica 1	Matemática Discreta y Lógica 2
	Matemática Discreta y Lógica 1 Introducción a la Programación	Estructuras de Datos y Algoritmos
	Matemática Discreta y Lógica 1 y Matemática Discreta y Lógica 2 Introducción a la Programación. Estructuras de Datos y Algoritmos.	Criptografía Aplicada
	Estructuras de Datos y Algoritmos.	Desarrollo Seguro de Aplicaciones
	Desarrollo Seguro de Aplicaciones	Taller de Programación segura
	Arquitectura de Sistemas Sistemas Operativos Introducción a la Programación	Redes de Computadoras
	Estructuras de Datos y Algoritmos Arquitectura de Sistemas Sistemas Operativos	Seguridad en Sistemas Operativos
	Redes de Computadoras	Seguridad en Redes de Computadoras
	Taller de Introducción a la Seguridad Informática	Taller de Técnicas y Procedimientos
	Redes de Computadores Seguridad en Redes Seguridad en Sistemas	Introducción al Análisis Forense Digital

	Operativos Seguridad de Aplicaciones	
	Sistemas Operativos Seguridad en Sistemas Operativos Redes de Computadoras Seguridad en Redes de Computadoras	Electivas: Configuración y Administración Segura de Sistemas
Evaluación	**RÉGIMEN DE APROBACIÓN:** Con derecho a "Exoneración": Todas las asignaturas	
	PASANTÍA Los estudiantes deberán tener aprobadas todas las asignaturas de los semestres I a IV y haber cursado todas las asignaturas del V semestre. El estudiante deberá realizar un informe sobre la pasantía, que será presentado por escrito al tutor referente quien deberá realizar la devolución en tiempo y forma para que pueda ser defendido de forma oral e individual.	
	PROYECTO FINAL Para la realización del mismo, los estudiantes deberán tener aprobadas todas las asignaturas de los semestres I a IV y haber cursado todas las asignaturas del V semestre. Tutor: el docente Orientador del Proyecto será el que dicte aquella disciplina que posea una relación importante con la temática del mismo. Trabajo: la elaboración podrá ser individual o en equipos con hasta un máximo de 3 integrantes. El Proyecto podrá iniciarse durante el año lectivo o con posterioridad al mismo.. El plazo máximo para realizar la Defensa es hasta 2 años, luego de la aprobación del curso (Art. 67 inc 3 y Art 72) En caso contrario se deberá iniciar un nuevo Proyecto (Art. 75). Tribunal: Estará integrado por el orientador y dos docentes de disciplinas relacionadas con la temática del trabajo.	
Observaciones.		

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		1			
UNIDAD CURRICULAR		Introducción a la Programación			
CRÉDITO EDUCATIVO		13			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 8		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

El objetivo de esta unidad curricular es presentar al estudiante conceptos básicos de programación en el paradigma de la programación imperativa. Luego de introducir elementos básicos de un lenguaje de programación, como C, se trabajará en el diseño, la implementación y el análisis de algoritmos simples (de pequeño porte).

Resultados de aprendizaje:

- Utiliza conceptos elementales de la programación imperativa, tales como: identificadores, variables, tipos de datos, estructuras de control y subprogramas (funciones y procedimientos).
- Diseña algoritmos para resolver problemas no complejos.
- Utiliza estructuras de control adecuadas para distintos problemas.
- Diseña algoritmos recursivos simples.
- Utiliza adecuadamente diferentes mecanismos de pasaje de parámetros en funciones y procedimientos.
- Construye programas o subprogramas de pequeño porte utilizando un lenguaje de programación imperativa, como C, contemplando aspectos tal como: codificación, compilación y depuración de errores.
- Identifica mejoras a la calidad de un código, basadas en la aplicación de buenas prácticas de diseño e implementación, y la ejecución de casos de prueba.
- Introduce y aplica nociones básicas de eficiencia en el diseño de soluciones.

Saberes estructurantes de la unidad curricular

1. Introducción a la computación a) Noción de algoritmo b) Lenguaje de programación: sintaxis y semántica c) Compilación y ejecución de programas.
2. Introducción a la programación imperativa a) Estructura de un programa b) Identificadores, constantes y variables c) Tipos de datos básicos d) Asignación y expresiones e) Entrada y salida
3. Algoritmo y estructuras de control a) Secuencia, selección e iteración b) Introducción a la recursión
4. Estructuras de datos a) Tipos primitivos b) Tipos estructurados

8

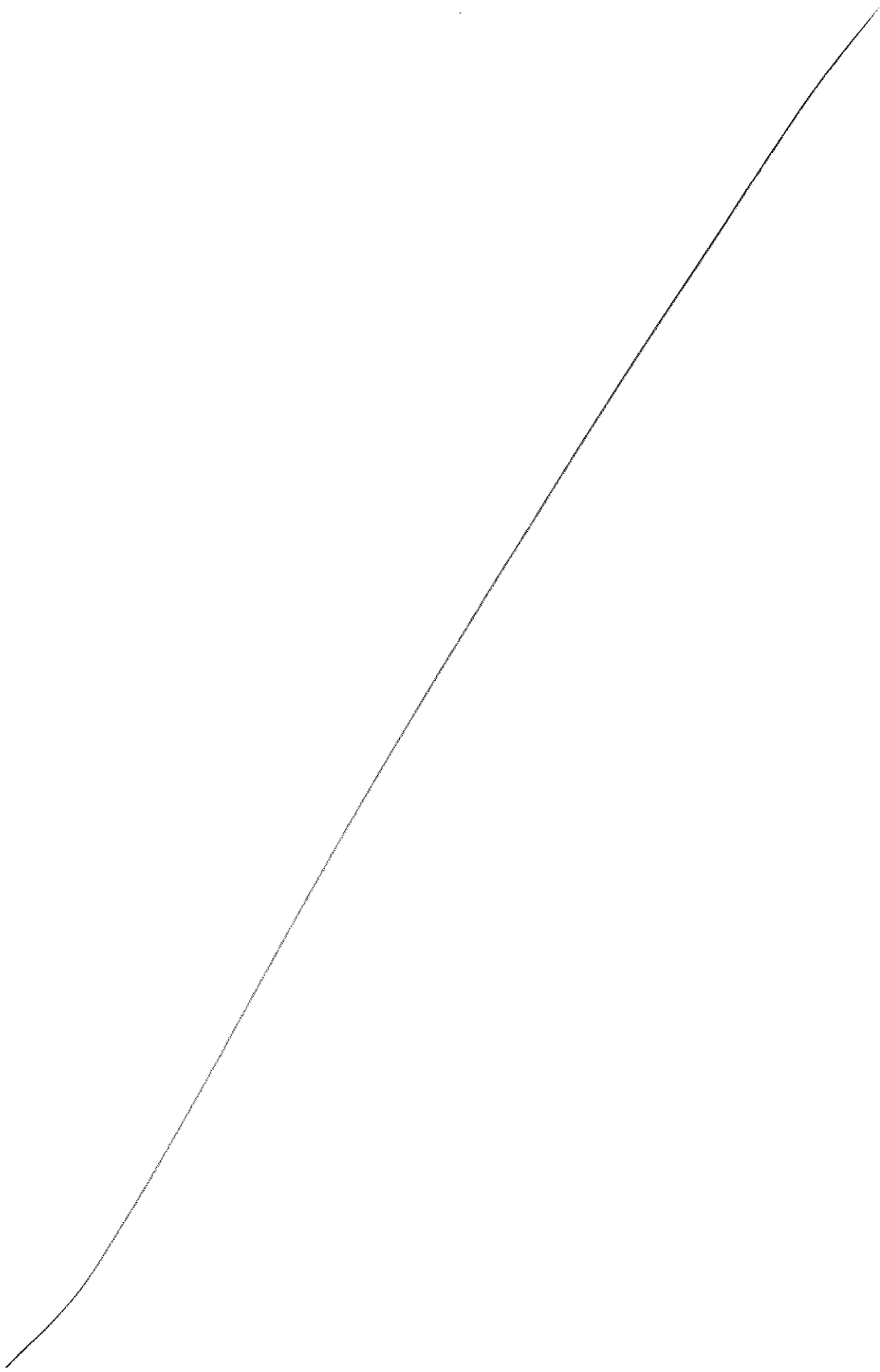
5. Descomposición y modularización a) Subprogramas (funciones y procedimientos) b)Especificación de operaciones mediante pre y post condiciones c) Pasajes de parámetro 6. Algoritmos de búsqueda y ordenación a) Búsquedas lineal y binaria b) Algoritmos de ordenación c) Análisis de estos algoritmos
7. Calidad y corrección a) Errores. Tipos de errores b) Buenas prácticas de diseño e implementación c) Nociones básicas de corrección de programas B.5.

Bibliografía Básica

B. W. Kernighan, D. M. Ritchie. El lenguaje de programación C. Prentice-Hall, (1991).

Complementaria

B. W. Kernighan, D. M. Ritchie. El lenguaje de programación C (Spanish Edition), (2021). 2. H. M. Deitel, P. J. Deitel. Cómo programar en C/C++. Prentice-Hall Hispanoamericana, (1998).



9

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		1			
UNIDAD CURRICULAR		Arquitectura de Computadoras			
CRÉDITO EDUCATIVO		8			
DURACIÓN DEL CURSO		Horas totales: 80	Horas semanales: 5		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

- Formar al estudiante para que maneje los conceptos básicos de la arquitectura de computadoras y el funcionamiento de sistemas computarizados.
- Capacitar al estudiante para que comprenda la arquitectura de sistemas y computadoras, tomando como base el modelo clásico de Von Neumann.
- Introducir al estudiante en temas de arquitecturas avanzadas y medidas de rendimiento.

Saberes estructurantes de la unidad curricular:

1. Introducción e historia de la arquitectura y organización de computadoras.
2. Sistemas de numeración y representación interna de datos.
3. Fundamentos de arquitectura de computadoras.
4. Compilación y código portable.
5. Comunicación e interconexión.
6. Arquitectura y organización del sistema de memoria.
7. Rendimiento basado en sistemas de microprocesador.
8. Modelos de sistemas distribuidos.

Analítica de los saberes estructurantes:

1. Introducción e historia de la arquitectura y organización de computadoras.

i. Indicar las razones por las que estudiar la arquitectura y organización de computadoras.

ii. Resaltar algunos hitos importantes en la historia de la computación.

iii. Indicar y explicar algunas áreas importantes como son organización y arquitectura de sistemas, memoria, interconexiones entre componentes, microprocesadores, y rendimiento.

iv. Contrastar los significados de organización de computadoras y arquitectura de computadoras.

v. Indicar la importancia de realizar aritmética binaria con computadoras.

vi. Indicar la importancia de medir correctamente el rendimiento.

Resultados de aprendizaje:

i. Identificar hitos importantes en la historia de la computación.

ii. Articular las diferencias entre organización y arquitectura.

iii. Identificar algunos componentes de una computadora.

iv. Describir como un tecnólogo usa o se beneficia con los conocimientos de arquitectura de computadoras.

2. Sistemas de numeración y representación interna de datos.

i. Sistemas posicionales.

ii. Sistemas con base.

iii. Algoritmos para conversión de base.

iv. Tipos de datos y sus representaciones: Caracter, String, Decimal, Moneda.

v. Representación de números enteros con y sin signo: Complemento a 1,complemento a 2.

vi. Algoritmos para operaciones aritméticas típicas.

vii. Importancia de rango, precisión y exactitud en la aritmética de computadoras.

viii. Representación de número reales, punto flotante (IEEE 754).

ix. Algoritmos para operaciones comunes con punto flotante.

Resultados de aprendizaje:

i. Conocer y entender cómo los valores numéricos son representados en computadoras digitales.

ii. Conocer y entender cómo los distintos tipos de datos son representados en computadoras digitales.

iii. Entender las limitaciones de la aritmética en computadoras y los efectos de errores en los cálculos.

3. Fundamentos de arquitectura de computadoras.

i. Organización y arquitectura de la máquina de von Neumann.

ii. Formatos de instrucción.

iii. El ciclo de instrucción.

iv. Registros.

v. Tipos de instrucción y modos de direccionamiento.

vi. Llamadas a subrutinas y mecanismos de retorno.

vii. Manejo de entrada/salida e interrupciones.

Resultados de aprendizaje:

i. Explicar la arquitectura de von Neumann y sus unidades funcionales.

ii. Explicar como una computadora realiza el fetch de memoria y ejecuta una instrucción.

iii. Articular las fortalezas y debilidades de la arquitectura de von Neumann.

4. Compilación y código portable:

i. Código fuente, código ensamblador, código objeto. Ejemplos.

ii. El compilador.

iii. Código portable y máquinas virtuales.

iv. Linkers y loaders.

Resultados de aprendizaje:

i. Identificar las diferencias entre código fuente y código binario.

ii. Explicar las tareas de un compilador.

iii. Explicar porqué existe código portable y código no portable.

iv. Describir el proceso desde que se escribe un programa hasta que este es ejecutado.

5. Comunicación e interconexión.

i. Fundamentos de entrada-salida: handshaking, buffering.

ii. Fundamentos de interrupciones.

iii. Técnicas de entrada-salida: E/S programada, E/S basada en interrupciones, DMA.

iv. Buses: protocolos y arbitraje.

Resultados de aprendizaje:

i. Describir cómo se realiza el acceso a datos desde dispositivos externos. Explicar cómo se usan las interrupciones para implementar E/S y transferencia de datos.

ii. Identificar los distintos tipos de buses en una computadora.

6. Arquitectura y organización del sistema de memoria.

i. Jerarquía de memoria.

ii. Codificación, compresión de datos e integridad de datos.

iii. Organización de la memoria principal y sus características y rendimiento.

iv. Métricas: latencia, tiempo de ciclo, ancho de banda e intercalado.

v. Memorias cache: mapeo de direcciones, tamaño de línea, reemplazos y políticas de escritura. vi. Tecnologías de memoria tales como DRAM, EPROM y FLASH.

11

Resultados de aprendizaje:

i. Identificar los principales tipo de tecnologías de memoria.

ii. Explicar los efectos de la latencia y ancho de banda de memoria en el rendimiento.

iii. Explicar el uso de la jerarquía de memoria para reducir la latencia de memoria.

7. Rendimiento basado en sistemas de microprocesador.

i. Métricas de rendimiento de computadoras: frecuencia del reloj, MIPS, ciclos por instrucción, benchmarks.

ii. Fortalezas y debilidades de las métricas de performance.

iii. El rol de la ley de Amdahl en el rendimiento de computadoras.

Resultados de aprendizaje:

i. Entender los factores que contribuyen al rendimiento de las computadoras.

ii. Entender las limitaciones de las métricas de rendimiento.

iii. Seleccionar la métrica de rendimiento más apropiada cuando se evalúan computadoras.

8. Modelos de sistemas distribuidos.

i. Clasificación de modelos: taxonomía de Flynn, clasificación de Handler.

ii. Niveles de paralelismo.

iii. Multiprocesadores y multicomputadores: topología, arquitecturas fuertemente acopladas y débilmente acopladas.

Resultados de aprendizaje:

Explicar la diferencia entre los diferentes paradigmas de paralelismo y su usabilidad y aplicabilidad.

Bibliografía

Computer Organization and Architecture: Designing for Performance, 8/E. William Stallings, PrenticeHall, 2010. ISBN-10: 0136073735, ISBN-13: 9780136073734.

Structured Computer Organization, 5/E. Andrew S. Tanenbaum, Prentice Hall, 2006. ISBN-10:0131485210, ISBN-13: 9780131485211

Computer System Architecture, 3/E. M. Morris Mano, Prentice Hall, 1993. ISBN-10: 0131755633, ISBN-13: 9780131755635.

12

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		1			
UNIDAD CURRICULAR		Matemática discreta y Lógica 1			
CRÉDITO EDUCATIVO		6			
DURACIÓN DEL CURSO		Horas totales: 64	Horas semanales: 4		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

El objetivo de esta unidad curricular es que el estudiante comprenda algunos conceptos básicos utilizados en informática para representar elementos de la realidad, pueda razonar y definir funciones sobre éstos. Asimismo, que el estudiante sepa utilizar elementos relevantes de matemática discreta y de lógica matemática, a nivel conceptual.

Resultados de aprendizaje:

- Reconoce la importancia de la modelización y abstracción en sistemas informáticos.
- Identifica y aplica los conceptos de conjunto, relación, función y secuencia, y reconocer su relevancia como herramientas de modelización en computación.
- Reconoce, interpreta y aplica diferentes tipos de pruebas matemáticas.
- Identifica, interpreta y aplica las ideas de conjunto inductivo, prueba por inducción (estructural) y función recursiva.
- Reconoce y aplica Máquina de Estados como herramienta de modelización para el análisis de procesos.
- Aplica definiciones y resultados básicos de combinatoria y teoría de grafos.
- Utiliza las técnicas de la matemática discreta para abordar problemas de conteo, numeración y combinación.
- Reconoce las nociones de conjuntos numerables y no numerables y su importancia en el contexto de la computación.

Saberes estructurantes de la unidad curricular:

1. Nociones sobre pruebas:
   a) Nociones de implicación, equivalencia, recíproco, inverso, contrarecíproco, negación y contradicción.
   b) Estructura de una prueba matemática.
   c) Pruebas directas, por contraejemplo y por absurdo.
2. Tipos de datos matemáticos:
   a) Conjuntos y secuencias.
   b) Funciones y relaciones binarias.
3. Definiciones inductivas y recursivas.
   a) Definición de conjuntos (lenguajes) inductivos.
   b) Pruebas por inducción estructural

13

c) Funciones recursivas.

4. Máquinas de estado
    a) Estados y transiciones.
    b) Análisis de corrección de algoritmos a través de máquinas de estados

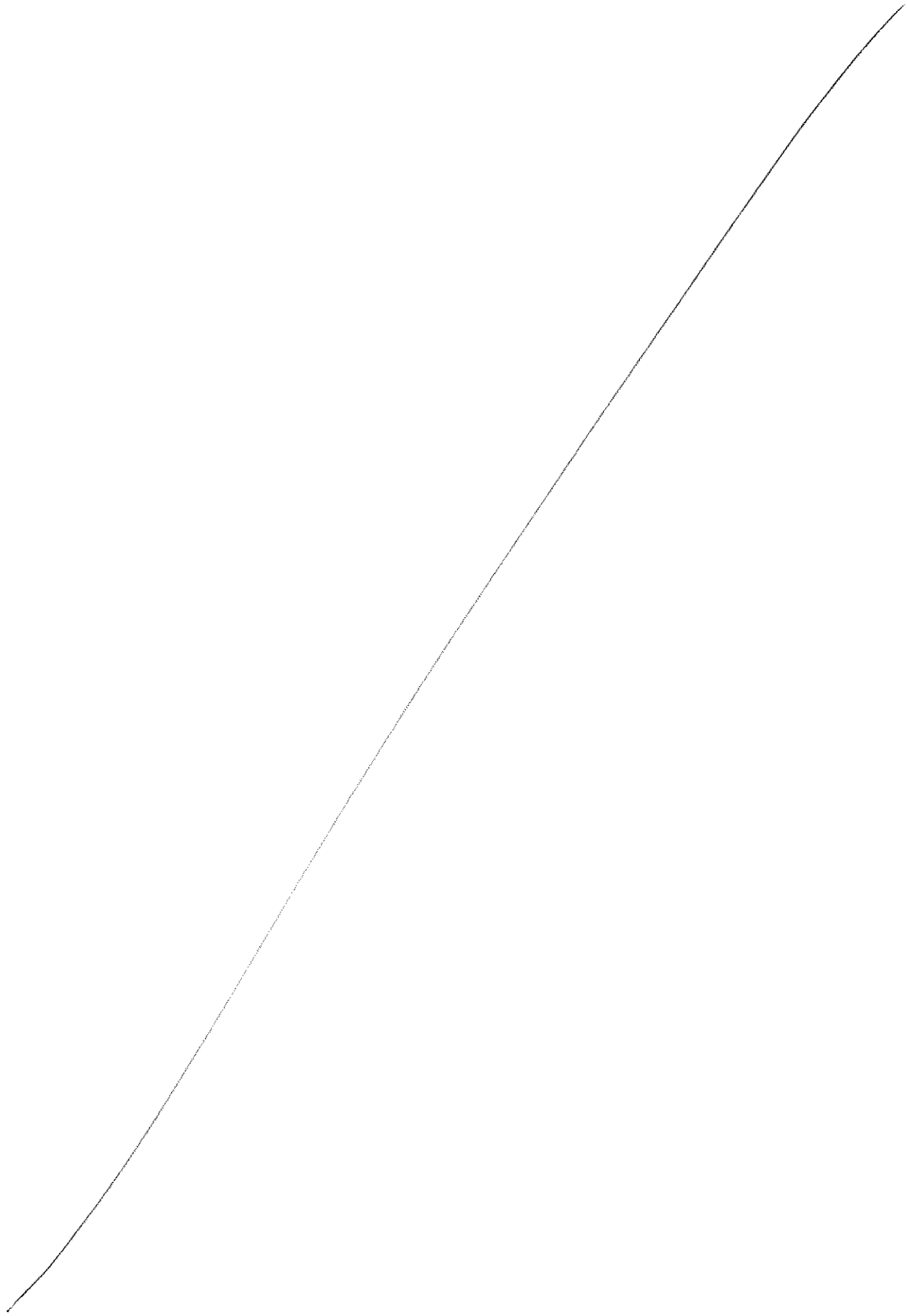
5. Grafos dirigidos y órdenes parciales:
    a) Grados de vértice, caminos.
    b) matrices de adyacencia, conteo de caminos.
    c) grafos acíclicos dirigidos, ordenamiento topológico.
6. Grafos simples:
    a) Adyacencia y grados de vértice.
    b) Grafos bipartitos y emparejamientos.
    c) Caminos, ciclos y conectividad
    d) Bosques y árboles
7. Combinatoria:
    a) Nociones básicas.
    b) Progresiones, permutaciones y combinaciones.
    c) Resolución de relaciones de recurrencia.

Bibliografía Básica

E. Lehman, F. Thomson Leighton, A. R. Meyer: Mathematics for Computer Science, (2017).

Complementaria

R. Grimaldi: Matemática discreta y combinatoria: Una introducción con aplicaciones, Addison-Wesley World Student Series, 3rd. Edition, (1998). 2. F. Moller, G. Struth: Modelling Computing Systems: Mathematics for Computer Science, (2013).



14

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		1			
ASIGNATURA			Taller de Introducción a la Seguridad Informática		
CRÉDITO EDUCATIVO		6			
DURACIÓN DEL CURSO		Horas totales: 64	Horas semanales: 4		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

Este curso se concibe como una aproximación inicial a la seguridad informática, para que los estudiantes que comienzan la carrera adquieran conceptos fundamentales de la ciberseguridad, reconozcan las características principales de esta disciplina y experimenten métodos y herramientas para la resolución de problemas concretos.

Saberes estructurantes de la unidad curricular:

1. Fundamentos de la Seguridad Informática:
    a) Motivación.
    b) Definiciones (confidencialidad, integridad y disponibilidad).
    c) Algunos tipos de ataques comunes y mecanismos de protección.
    d) Introducción a la privacidad y protección de datos personales.

2. Talleres:
    Ejes temáticos:
    a) Conceptos básicos de criptografía, motivación, definiciones y algunas herramientas.
    b) Manejo elemental de consola y comandos básicos, scripting.
    c) Programación web básica (HTML, CSS, javascript)
    d) Uso básico de algunas herramientas de seguridad (nmap, tcpdump, ettercap, netcat, curl/wget, john the ripper, zap, etc).

Sugerencias metodológicas:

El curso cubre los fundamentos y propiedades básicas de seguridad informática (como confidencialidad, integridad y disponibilidad), y los principales tipos de ataques de los que puede ser objeto un sistema informático, así como los posibles métodos de protección, detección y políticas de seguridad que permitan evitar el daño al sistema o minimizar sus consecuencias. Complementando el contenido teórico, se brindarán una serie de talleres durante los cuales los estudiantes realizarán actividades en equipo que ilustren y permitan experimentar técnicas y herramientas de ciberseguridad concretas. Estos talleres tendrán una metodología de enseñanza activa y con sesgo lúdico. Se pueden realizar actividades

competitivas, como capturas de bandera en escenarios sencillos, en donde los propios equipos pueden esconder cierta bandera en un ambiente, y a la vez descubrir la de otros grupos, lo que permite desempeñar roles tanto ofensivos como defensivos. El objetivo principal de este taller es motivar a los estudiantes en el estudio de la ciberseguridad, por lo que se recomienda que las actividades de taller (y por lo tanto los temas que se aborden en esta segunda parte del curso) sean elegidas contemplando en la medida de lo posible los intereses de los estudiantes.

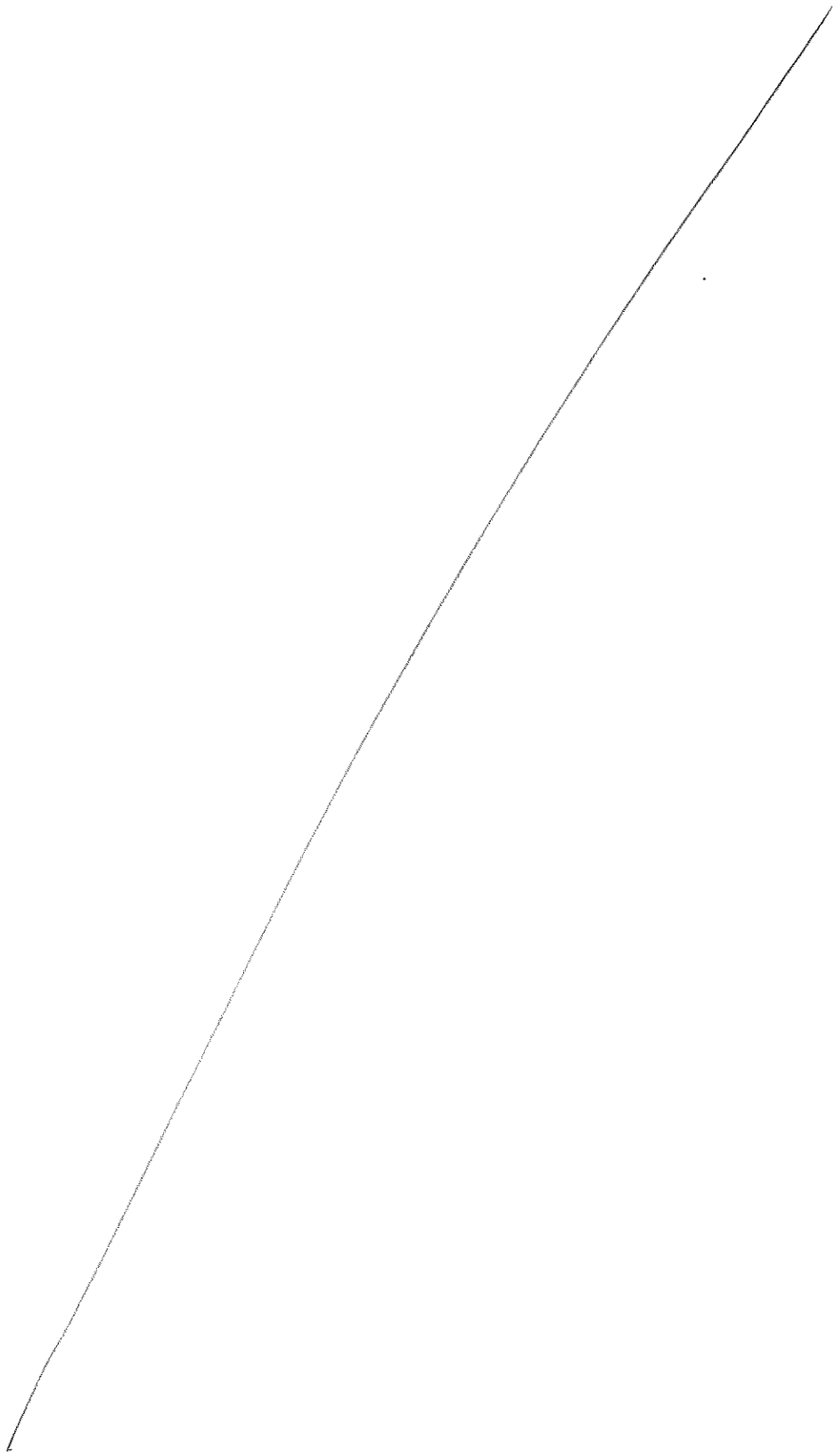
Bibliografía

Básica

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

Complementaria

Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), AGESIC; Materiales Didácticos (videos, afiches, juegos y otras actividades) de la campaña "Seguro te conectás"; https://www. gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/ ciudadania.



16

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		2			
UNIDAD CURRICULAR		Estructura de Datos y Algoritmos			
CRÉDITO EDUCATIVO		13			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 8		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

El objetivo de esta unidad curricular es introducir estructuras de datos básicas y sus algoritmos de manipulación, realizar un análisis de su eficiencia, e introducir el concepto de abstracción de datos para el diseño y la evaluación de algoritmos de porte mediano.

Resultados de aprendizaje:

- Implementa y analiza algoritmos recursivos.
- Define y manipula estructuras de datos lineales y arborescentes, tanto estáticas como dinámicas.
- Reconoce los conceptos de modularización, abstracción de datos, encapsulamiento y Tipo Abstracto de Datos (TAD).
- Explica la diferencia entre especificación, implementación y uso de TADs.
- Especifica diferentes TADs y ejemplifica su uso. Por ejemplo: Lista, Pila, Cola de Prioridad, Conjunto, Mapping y Grafo. Implementar TADs usando estructuras de datos, por ejemplo arreglos, estructuras de datos lineales y arborescentes de memoria dinámica, tablas de dispersión y árboles parcialmente ordenados.
- Escoge estructuras de datos adecuadas para implementar los TADs teniendo en cuenta requerimientos de eficiencia en tiempo de ejecución y espacio de almacenamiento.
- Define nociones de eficiencia para aplicarlas al análisis de los algoritmos de las estructuras vistas. Identificar qué TADs se vinculan con la resolución de ciertos problemas.

Saberes estructurantes de la unidad curricular:

1. Iteración y recursión a) Implementación de invocaciones a procedimientos y funciones b) Implementación y uso de esquemas recursivos c) Análisis comparativo entre algoritmos recursivos e iterativos

2. Introducción al análisis de algoritmos a) Eficiencia en espacio de almacenamiento y tiempo de ejecución b). Tiempo de ejecución y orden del peor caso de algoritmos iterativos y recursivos c) Introducción al análisis del caso promedio

3. Estructuras de datos estáticas y dinámicas a) Estructuras de datos lineales. Distintos tipos de listas b) Estructuras de datos arborescentes. En particular, árboles binarios, binarios de búsqueda, árboles balanceados y árboles generales c) Tablas de dispersión (hashing) d) Montículos binarios (binary heap) e) Implementación de estructuras múltiples para resolver

17

problemas con restricciones de eficiencia

4. Tipos abstractos de datos (TADs) a) El rol de la abstracción en el diseño de sistemas b) Especificación e implementación de TADs Distintos tipos de listas, pilas y colas Conjuntos, multiconjuntos, funciones parciales (mappings, tablas) y colas de prioridad Grafos c) Uso de TADs en la resolución de problemas de porte mediano.

Bibliografía

Básica

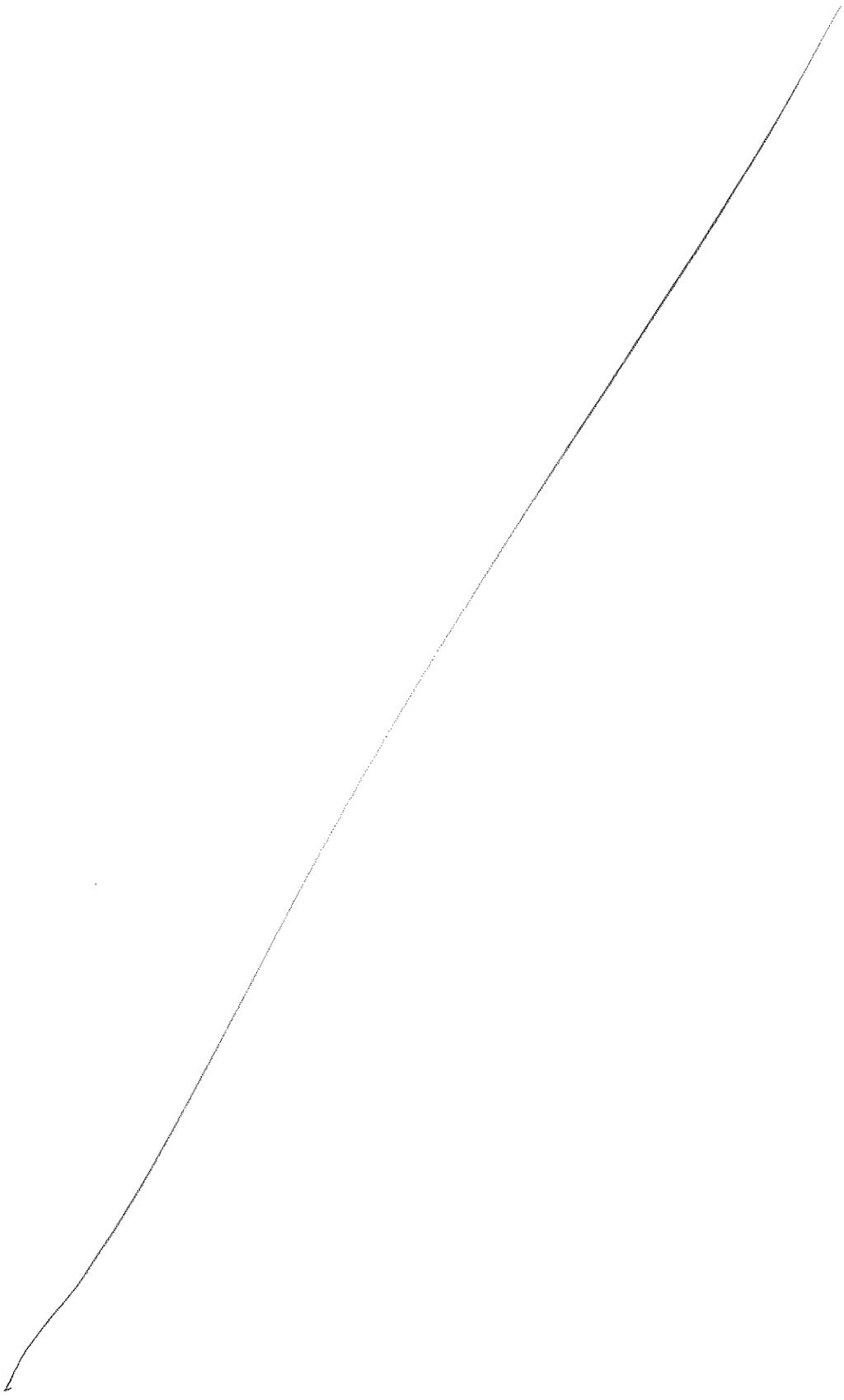
Mark A. Weiss. Data Structures and Algorithm Analysis in C (2nd Edition), (1996).

Complementaria

B. W. Kernighan, D. M. Ritchie. El lenguaje de programación C (Spanish Edition), (2021).

H. M. Deitel, P. J. Deitel. Cómo programar en C/C++. Prentice-Hall Hispanoamericana, (1998).

G. Brassard, P. Bratley. Fundamentos de Algoritmia. Prentice Hall, (1998).



10

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		2			
UNIDAD CURRICULAR			Sistemas Operativos		
CRÉDITO EDUCATIVO		8			
DURACIÓN DEL CURSO		Horas totales: 80	Horas semanales: 5		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

El objetivo de este curso es introducir conceptos fundamentales de seguridad en Sistemas Operativos. Se presentan tanto amenazas específicas y tipos de ataque como mecanismos de identificación y autenticación. Se pone particular énfasis en la gestión de contraseñas y en la implementación de los mecanismos de control de acceso y de auditoría provistos por los sistemas operativos. Se presenta el concepto de computación confiable y de seguridad multinivel.

Resultados de aprendizajes:

- Discute los cuatro métodos generales para autenticar la identidad de un usuario.
- Explica el mecanismo mediante el cual se utilizan contraseñas hash para la autenticación de usuarios.
- Presenta una descripción general de la autenticación de usuarios basada en tokens.
- Explica cómo se ubica el control de acceso en el contexto más amplio que incluye autenticación, autorización y auditoría.
- Distingue entre sujetos, objetos y derechos de acceso.
- Discute los conceptos principales del control de acceso basado en roles y el basado en atributos. Enumerar los pasos necesarios en el proceso de aseguramiento de un sistema.
- Enumera los pasos básicos utilizados para asegurar el sistema operativo base.
- Explica algunos aspectos específicos de la seguridad de los sistemas Unix/Linux.
- Explica algunos aspectos específicos de la seguridad de los sistemas Windows.
- Enumera los pasos necesarios para mantener la seguridad en los sistemas virtualizados.
- Explica el modelo Bell-LaPadula y su relevancia para la computación confiable.
- Resume otros modelos formales de seguridad informática.
- Comprende el concepto de sistemas confiables.
- Enumera y explica las propiedades de un monitor de referencia y las relaciones entre un monitor de referencia y una base de datos del kernel de seguridad.
- Logra presentar una descripción general de la aplicación de la seguridad multinivel al control de acceso basado en funciones.

Saberes estructurantes de la unidad curricular:

1. Autenticación:

    a) Principios de autenticación de usuario.

    b) Autenticación de usuarios basada en secretos y en tokens.

    c) Mecanismos biométricos.

    d) Autenticación remota.

2. Control de acceso:

    a) Principios de control de acceso.

    b) Sujetos, objetos y permisos.

    c) Control de acceso discrecional (DAC).

    d) Control de acceso basado en roles (RBAC).

    e) Control de acceso basado en atributos (ABAC).

    f) Gestión de identidades, credenciales y de acceso.

3. Seguridad de Sistemas Operativos:

    a) Planificación de la seguridad de SO y Hardening.

    b) Mantenimiento: Logging y Backup.

    c) Seguridad Linux/Unix.

    d) Seguridad Windows.

    e) Seguridad de sistemas de virtualización.

4. Computación confiable y Seguridad Multinivel:

    a) El modelo Bell-LaPadula para seguridad computacional.

    b) Otros modelos.

    c) El concepto de modelo confiable.

    d) Aplicaciones de seguridad multinivel.

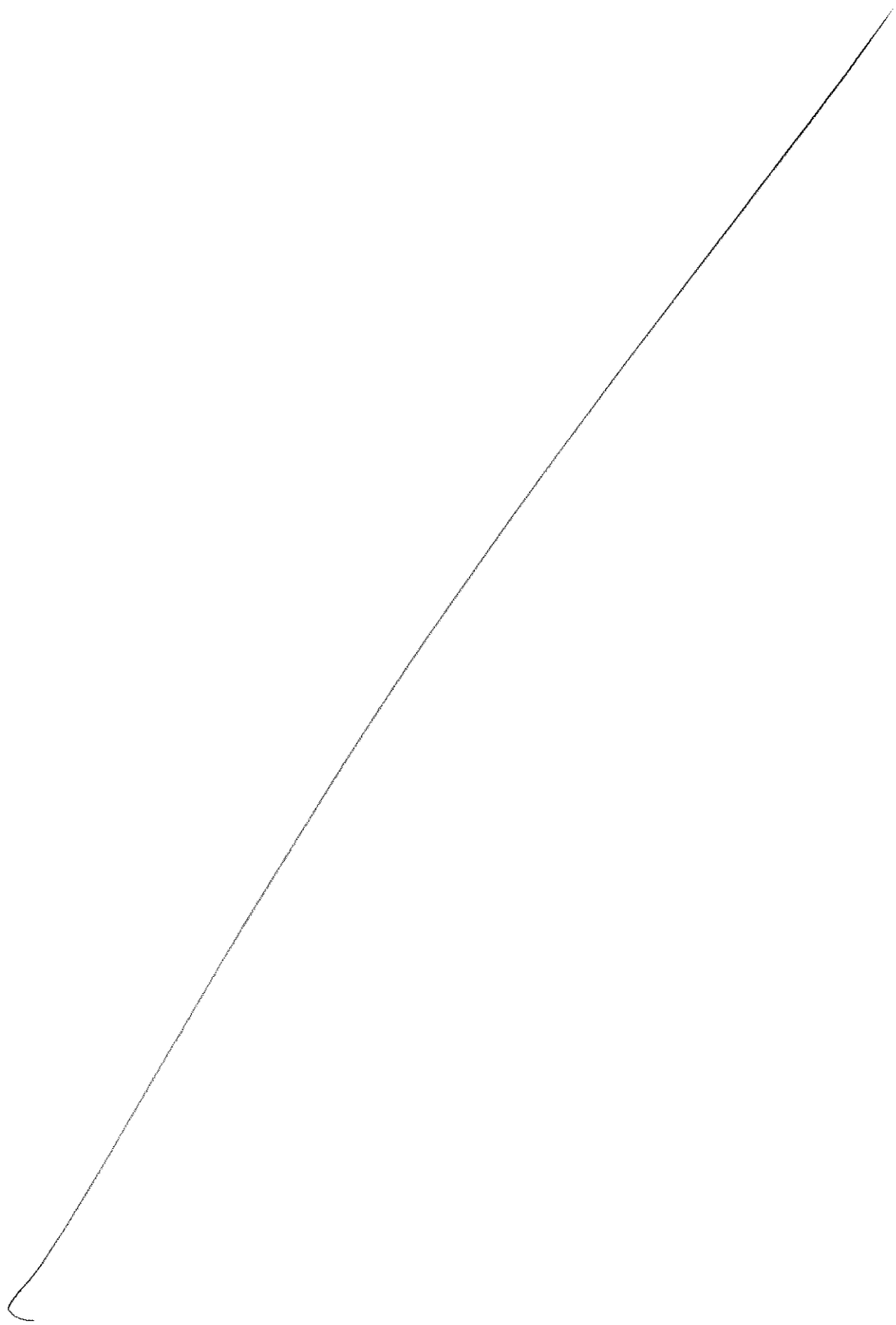
Bibliografía

Básica

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

Complementaria

Gollman, Dieter (2009), Computer Security, Wiley Computing Publishing, 3rd. Editon. J.6.



20

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		2			
ASIGNATURA		Matemática discreta y Lógica 2			
CRÉDITO EDUCATIVO		6			
DURACIÓN DEL CURSO		Horas totales: 64	Horas semanales: 4		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2028	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

El objetivo de esta unidad curricular es que el estudiante comprenda la Lógica de Predicados desde el punto de vista formal y como mecanismo de especificación y verificación. Asimismo, que sepa utilizar elementos relevantes de matemática discreta y de lógica matemática para formalizar elementos de la realidad.

Resultados de aprendizaje:

- Reconoce los componentes de un sistema formal.
- Interpretar y distinguir las nociones de verdad, juicio y fórmula lógica en Lógica de Primer Orden.
- Interpretar y distinguir elementos sintácticos de la Lógica de Primer Orden.
- Interpretar la noción de estructura de primer orden.
- Interpretar y diferenciar los juicios que involucran fórmulas, términos y estructuras.
- Construir estructuras y lenguajes de primer orden adecuados para representar una realidad determinada.
- Identificar y probar propiedades sintácticas de los lenguajes de primer orden. Identificar y probar propiedades algebraicas de la Lógica de Primer Orden.
- Interpretar las reglas de inferencia de Deducción Natural como esquemas de razonamiento típicos de las matemáticas.
- Construir pruebas usando las reglas de Deducción Natural.
- Interpretar y aplicar las ideas de axioma, teorema, teoría lógica, consistencia.
- Interpretar las nociones de corrección y completitud de la lógica clásica de primer orden.

Saberes estructurantes de la unidad curricular

1. Sintaxis de la Lógica de Primer Orden (LPO) a) Definición de estructura de primer orden b) Definición recursiva de términos y fórmulas sobre un alfabeto c) Definición de variables libres, ligadas, sustituciones
2. Semántica de la LPO a) Interpretaciones sobre estructuras. Definición recursiva de funciones de interpretación b) Interpretación recursiva de fórmulas proposicionales. Definición de Tautología, Contingencia y Contradicción c) Interpretación de fórmulas de

21

primer orden. Clausura Universal. Definición de juicios: Satisfactible, Lógicamente Válido y Consecuencia Lógica d) Propiedades algebraicas básicas, equivalencia, teoremas de cambios de variables y de sustitución. Identidad e) Formalización y análisis de propiedades sobre distintas realidades

3. Deducción Natural en LPO a) Reglas de derivación y heurísticas b) Definición inductiva del lenguaje de las derivaciones c) Análisis de casos de estudio

4. Corrección y Completitud de la LPO a) Nociones de corrección y completitud del sistema de pruebas b) Corrección del sistema c) Conjuntos consistentes e inconsistentes. Definición de teoría d) Noción de conjunto completo y consistencia maximal

Bibliografía

Básica

D. van Dalen: Logic and Structure. Springer London, 5th Edition, (2013).

Complementaria

H. B. Curry: Foundations of mathematical logic. Dover Publications, 2nd Edition, (2010).

E. Lehman, F. Thomson Leighton, A. R. Meyer: Mathematics for Computer Science, (2017).

22

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		2			
UNIDAD CURRICULAR		Inglés Técnico			
CRÉDITO EDUCATIVO		6			
DURACIÓN DEL CURSO		Horas totales: 64	Horas semanales: 4		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Propósitos de la unidad curricular:

La ciberseguridad se ha convertido en una área que ha cobrado relevancia dentro de las TI en la actualidad ya que es de vital importancia minimizar el nivel de riesgo al que está expuesta la información, ante amenazas o incidentes cibernéticos. El objetivo de la seguridad informática es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por computadora.

En este contexto, la evolución constante del mundo moderno y el desarrollo vertiginoso de las telecomunicaciones a nivel mundial y la globalización, conlleva a que el idioma inglés esté presente en el campo académico y profesional. Esta presencia a nivel global demanda la utilización de este idioma como vehículo de comunicación universal en el siglo XXI. En consecuencia, el conocimiento de la lengua inglesa se impone como un requisito indispensable para estudiantes, docentes, investigadores y profesionales que necesitan información completa, actualizada y veraz que les permita el descubrimiento de nuevos saberes, reflexionar acerca de los problemas de seguridad y cómo la lengua meta puede contribuir a minimizar su impacto.

A través de la unidad curricular Inglés Técnico, se pretende proporcionar al estudiante las competencias básicas para insertarse en el mundo de hoy, para que éstos comprendan las distintas situaciones, resuelvan problemas y tomen decisiones. El dominio de la lengua inglesa integra una de esas competencias puesto que es el código predominante en los ámbitos laborales y/o académicos, que no sólo le permite al educando su desarrollo cognitivo, sino el mejor conocimiento de su lengua materna.

En el transcurso de la unidad curricular, se trabajarán las competencias y estrategias para comprender textos académicos e interactuar en inglés, aspectos fundamentales para un desempeño eficaz en el mundo de las TIC. El inglés es el idioma más comúnmente empleado en la publicación de trabajos, en congresos, seminarios internacionales y en el mundo de la tecnología y la computación. Por ende, esta unidad curricular cobra importancia dentro de la currícula porque permite al futuro egresado acceder a fuentes de información de su interés de primera mano, conociendo y evaluando bibliografía publicada en lengua inglesa. A su vez, amplía su horizonte de conocimientos al investigar, comprender manuales, seguir instrucciones, leer páginas web e interactuar en inglés.

En síntesis, Inglés Técnico le permitirá al estudiante fortalecer las macrohabilidades de la lengua con el fin de favorecer una comunicación de forma efectiva en contextos diversos y complejos. Las actividades que el docente desarrolle debe atender a los procesos cognitivos específicos del estudiante en relación a la lengua meta (L2): hablar, escuchar, leer, escribir y la reflexión metalingüística.

Resultados de aprendizaje:

- Resuelve problemas mediante proyectos integrados de indagación personales y colaborativos mediados por la tecnología.
- Desarrolla habilidades, identifica conflictos y visualiza soluciones.
- Comprende e integra el lenguaje técnico-tecnológico en la lengua extranjera.
- Busca soluciones a problemas de distinta índole utilizando las herramientas digitales a su alcance.
- Conoce la administración de equipos de hardware, su mantenimiento y aseguramiento físico.
- Comprende la importancia de la ciberseguridad y reflexiona acerca de ella.
- Reconoce diferentes arquitecturas de red y sus efectos en la ciberseguridad.
- Reconoce e identifica las tecnologías de virtualización y servicios en la nube.
- Comprende las capacidades de la computación en la nube.
- Describe las posibles amenazas en la red y la forma de contrarrestar las mismas.
- Establece comparaciones entre los diferentes tipos de ciberataques.
- Explica los distintos servicios en línea.
- Identifica las distintas formas en las cuáles un sistema puede verse en riesgo de ciberataque.
- Reconoce las tendencias actuales en técnicas de ciberataque
- Identifica los conceptos básicos de los principales procesos y respuestas ante incidentes.
- Identifica y establece comparaciones entre las diferentes técnicas criptográficas.
- Reconoce las normas que los estados están creando para la protección de la información y los datos.

Saberes estructurantes de la unidad curricular:

Thematic Unit 1: What is cybersecurity?
Se detallan a continuación los temas a abordar dentro de la unidad temática. A partir de la unidad el docente podrá a su vez trabajar con temas de interés que surjan por parte de los estudiantes. Los temas son los siguientes: • Cybersecurity definition and use • The Internet of things • Impact of cybersecurity • The CIA triad
Contenidos: • Definición de ciberseguridad • Acrónimos • Internet de las cosas • Confidencialidad, Integridad y Accesibilidad (CIA)

Thematic Unit 2: The ABCs of cryptography
Se detallan a continuación los temas a abordar dentro de la unidad temática. A partir de la unidad el docente podrá a su vez trabajar con temas de interés que surjan por parte de los estudiantes. Los temas son los siguientes: • Cryptology, cryptography and cryptanalysis • Why is encryption important? • Basic crypto systems • Advanced cryptography
Contenidos: • Diferencia entre criptología, criptografía y criptoanálisis • Sistemas de encriptación • Encriptación y desencriptación • Avances en el área de la criptografía

Thematic Unit 3: Software security
Se detallan a continuación los temas a abordar dentro de la unidad temática. A partir de la unidad el docente podrá a su vez trabajar con temas de interés que surjan por parte de los estudiantes. Los temas son los siguientes: • Common security problems • Databases security • SQL injection, types of SQLi and prevention • Hardening
Contenidos: • Problemas en el área de la seguridad • Bases de datos y seguridad de los mismos • Inyección SQL, tipos de infiltración de código intruso y su prevención • Proceso de reducción de vulnerabilidades.

Estrategias metodológicas:

Los contenidos se deben trabajar en base a temas. El marco ideal para el desarrollo de los temas son las unidades temáticas, partiendo de un tema general relacionado con la orientación del curso. El docente jerarquizará aquellos temas de cada unidad para trabajar en forma particular de acuerdo a las características del grupo y a los acuerdos logrados con los docentes del curso. El docente diseñará y secuenciará las actividades que considere adecuadas para el logro de los objetivos del curso, teniendo en cuenta que el estudiante adquiera las competencias lingüísticas y comunicativas necesarias.

El docente al enseñar deberá ser ecléctico lo que implica escoger las estrategias de enseñanza que mejor se ajusten a las necesidades e intereses de los estudiantes.

Evaluación

La evaluación se realizará de acuerdo al reglamento vigente. No obstante, conviene destacar que la evaluación, concebida como parte del proceso de enseñanza y de aprendizaje, debe ser continua y fundamentalmente formativa. Se sugiere la incorporación de diferentes técnicas, instrumentos y herramientas para la recolección de información sobre los aprendizajes de los

estudiantes y sus singularidades, y que permitan tomar decisiones fundamentadas al docente. Asimismo, se sugiere desarrollar las instancias de evaluación en distintos formatos.

Bibliografía de referencia para el docente

Angel M.Y. Lin (2016). *Language Across the Curriculum & CLIL in English as an Additional Language (EAL) Contexts*. Springer Science+Business Media

Anthony, L. (2018). *Introducing English for Specific Purposes*. Routledge.

Clark, K. (2022) *Cybersecurity for Beginners*

Cornish, P (2022) *The Oxford Handbook of Cyber Security*

Dauti, D. (2022). *Windows Server 2022 Administration Fundamentals.* Packt. 3rd Edition.

Du, W. (2022). *Computer Security: A Hands-on Approach (Computer & Internet Security).* Syracuse University. 3rd Edition.

Gregory, G. & Chapman, C. M. (2013). *Differentiated Instruction Strategies: One size does not fit all.* Corwin Press.

Harding, K. (2007). *English for Specific Purposes*. Oxford University Press.

Hein, T., Nemeth, E., Snyder, G., Whaley, B., & Mackin, D. (2017). *UNIX and Linux System Administration Handbook.* Addison-Wesley Professional. 5th Edition.

Julian, M. (2017). *Practical Monitoring: Effective Strategies for the Real World.* O'Reilly. 1st Edition.

Kim, G., Debois, P., Willis, J., & Humble, J. (2021). *The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations.* IT Revolution Press. 2nd Edition.

Lightbown, P., & Spada, N. M. (2017). *How languages are learned.* Oxford University Press.

Paar, C., Pelzl, J., Preneel, B. (2014). *Understanding Cryptography: A Textbook for Students and Practitioners.* Springer. 10th Edition.

25

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		2			
UNIDAD CURRICULAR		Introducción a las Bases de Datos			
CRÉDITO EDUCATIVO		6			
DURACIÓN DEL CURSO		Horas totales: 64	Horas semanales: 4		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivo de la Asignatura

- Diseñar, crear y administrar bases de datos relacionales de mediano porte.
- Incrementar el poder de abstracción en la representación de datos.
- Buscar distintas soluciones para un mismo problema y ser capaz de seleccionar la más adecuada.
- Integrar los conocimientos adquiridos en esta asignatura con otras.

Resultados de aprendizaje:

Diseña e implementa una Base de Datos relacional, así como también de generar consultas sencillas a la misma.

Saberes estructurantes de la unidad curricular:

UNIDAD I: Introducción

- Conceptos Generales de:
- Bases de Datos.
- Sistemas de Base de Datos.
- Sistemas de Gestión de Bases de Datos.
- Modelos de datos.
- Fases en el diseño de Bases de Datos.

UNIDAD II: Modelo de Datos conceptual: Modelo Entidad Relación

- Conceptos generales
- Introducción a diagramas entidad relación

UNIDAD III: Modelo de Datos de implementación.

- Modelo relacional
- Conceptos generales
- Restricciones:
- de dominio
- de clave
- de integridad
- de entidades

- referencial
- claves externas
- Creación y modificación de relaciones

UNIDAD IV: Lenguajes para SGBD relacionales.

- Presentación general
- SQL
- Definición de datos (D.D.L)
- Manejo de datos (D.M.L)
- Consultas
- Actualización.

UNIDAD V: Diseño de BD relacionales.

- Conceptos generales
- Pautas para el diseño de esquemas
- Dependencias funcionales
- Formas normales
- Pasaje del modelo entidad-relación al modelo relacional

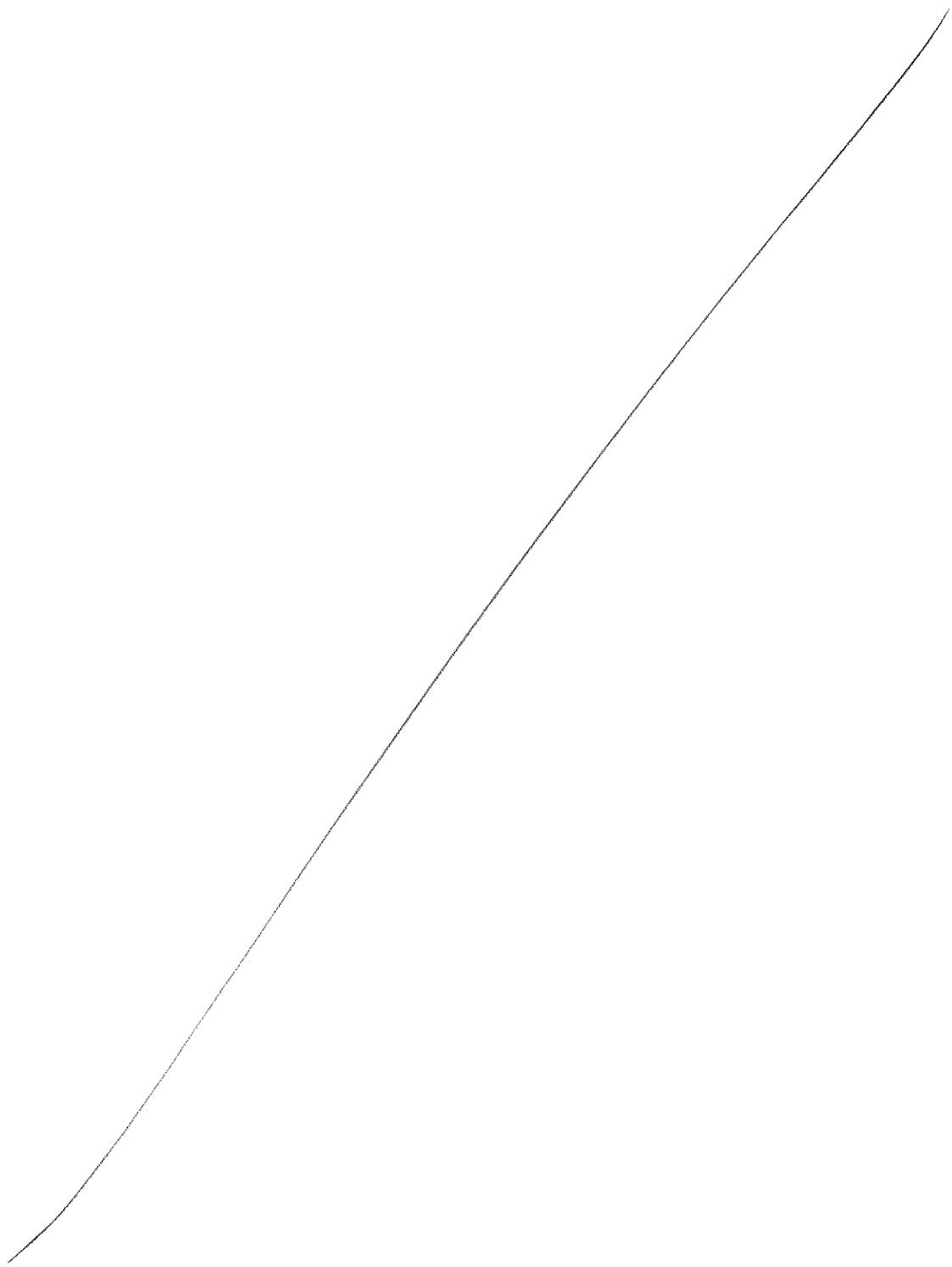
Bibliografía

Elmasri, R. & Navathe, S. , Fundamentals of Database Systems.

Ullman, J. & Widom, J., A first course in Database Systems.

Ullman, J., Principles of Database and Knowledge-base Systems.

Date, C.J., An introduction to Database Systems. Ed. Prentice-Hall.



27

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		2			
SEMESTRE/ MÓDULO		3			
UNIDAD CURRICULAR		Desarrollo seguro de aplicaciones			
CRÉDITO EDUCATIVO		13			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 8		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos

El objetivo de esta unidad curricular es introducir los principales conceptos y metodologías asociadas a la seguridad en el desarrollo de aplicaciones. Se presentan y discuten amenazas específicas al dominio, poniendo especial énfasis en técnicas para el diseño seguro de aplicaciones, la validación y sanitización de datos de entrada.

Saberes estructurantes de la unidad curricular:

- Requerimientos y estándares de seguridad.
- Arquitectura y diseño.
-
    - Modelado de amenazas.
    - Características de seguridad y diseño.
    - Análisis de arquitectura.
- Código.
    - Revisión de código - automatización.
    - Gestión de Dependencias.
- Testing:
    - Testing de seguridad.
- Despliegue y mantenimiento:
    - Test de penetración.
    - Gestión de configuración y vulnerabilidades.

Bibliografía:

Básica

D. Fisher, Application Security Program Handbook, 2022. 2. L. Bell, M. Brunton-Spall, R. Smith, J. Bird, Application Security: Enabling Security in a Continuous Delivery Pipeline, 2017. 3. OWASP ASVS, https://github.com/OWASP/ASVS/.

Complementaria

BSIMM Framework, https://www.bsimm.com/content/dam/bsimm/reports/bsimm12-foundations.pdf.

NIST, Secure Software Development Framework SSDF, https://csrc.nist.gov/Projects/ssdf.

OWASP SAMM, https://owaspsamm.org.

OWASP Top 10, https://owasp.org/www-project-top-ten/.

SANS Top 25 software errors, https://www.sans.org/top25-softwareerrors/.

28

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		2			
SEMESTRE/ MÓDULO		3			
UNIDAD CURRICULAR		Redes de computadoras			
CRÉDITO EDUCATIVO		8			
DURACIÓN DEL CURSO		Horas totales: 80	Horas semanales: 5		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

El objetivo de esta unidad curricular es introducir al estudiante en los conceptos de comunicación de datos en redes de computadoras. Se estudian los modelos de referencia OSI y TCP/IP, y las funcionalidades de cada capa. Se presentan los principales protocolos en la capa de aplicación (DNS, SMTP, HTTP, etc.), en la capa de transporte (TCP y UDP), en la capa de red (IPv4, IPv6, ICMP), y en la capa de enlace (ethernet, arp). Adicionalmente, se presentan conceptos básicos de las redes inalámbricas (WiFi).

Saberes estructurantes de la unidad curricular:

1. Introducción.

a) Introducción general a los temas del curso.

b) Modelos de circuitos virtuales y de datagramas.

c) Presentación del modelo de capas OSI de ISO y TCP-IP.

2. Capa de aplicación.

a) Presentación de aplicaciones tradicionales que dan soporte a Internet (DNS, SMTP, HTTP, entre otras)

b) Modelos Cliente-Servidor y Peer-to-Peer.

3. Capa de transporte.

a) Servicios ofrecidos a la capa superior

b) Comunicación extremo a extremo entre procesos, multiplexación, interfaz de programación de sockets.

c) Transporte confiable y no confiable.

d) Funcionamiento del User Datagram Protocol (UDP) y del Transport Control Protocol (TCP).

4. Capa de red.

a) Servicios ofrecidos a la capa superior.

b) Comunicación extremo a extremos entre sistemas, enrutamiento y reenvío.

c) Descripción del Internet Protocol (IP).

d) Subredes y numeración.

e) Algoritmos de enrutamiento de vector-distancia y de estado del enlace.

f) Enrutamiento jerárquico, comunicaciones broadcast y multicast.

g) Protocolo IPv6.

5. Capa de enlace.

a) Servicios ofrecidos a la capa superior.

b) Comunicación entre vecinos, detección y corrección de errores.

c) Medios punto a punto y medios compartidos.

d) Direcciones de capa de enlace, redes de área local.

Bibliografía

J. Kurose, K. Ross; Redes de Computadoras: Un Enfoque Descendente; Ed. Pearson; 7th Edition (2017).

A. Tanenbaum; Computer Networks; 5th Edition (2010). 2. D. Comer; Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture; 5th Edition (2005).

30

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		2			
SEMESTRE/ MÓDULO		3			
UNIDAD CURRICULAR		Seguridad de sistemas Operativos			
CRÉDITO EDUCATIVO		13			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 8		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos

El objetivo de este curso es introducir conceptos fundamentales de seguridad en Sistemas Operativos. Se presentan tanto amenazas específicas y tipos de ataque como mecanismos de identificación y autenticación. Se pone particular énfasis en la gestión de contraseñas y en la implementación de los mecanismos de control de acceso y de auditoría provistos por los sistemas operativos. Se presenta el concepto de computación confiable y de seguridad multinivel.

Resultados de aprendizaje:

- Discute los cuatro métodos generales para autenticar la identidad de un usuario.
- Explica el mecanismo mediante el cual se utilizan contraseñas hash para la autenticación de usuarios.
- Presenta una descripción general de la autenticación de usuarios basada en tokens.
- Explica cómo se ubica el control de acceso en el contexto más amplio que incluye autenticación, autorización y auditoría.
- Distingue entre sujetos, objetos y derechos de acceso.
- Discute los conceptos principales del control de acceso basado en roles y el basado en atributos.
- Enumera los pasos necesarios en el proceso de aseguramiento de un sistema. Enumerar los pasos básicos utilizados para asegurar el sistema operativo base.
- Explica algunos aspectos específicos de la seguridad de los sistemas Unix/Linux.
- Explicar algunos aspectos específicos de la seguridad de los sistemas Windows.
- Enumera los pasos necesarios para mantener la seguridad en los sistemas virtualizados. Explica el modelo Bell-LaPadula y su relevancia para la computación confiable.
- Resume otros modelos formales de seguridad informática.
- Comprende el concepto de sistemas confiables.
- Enumera y explica las propiedades de un monitor de referencia y explicar las relación entre un monitor de referencia y una base de datos del kernel de seguridad.
- Presenta una descripción general de la aplicación de la seguridad multinivel al control de acceso basado en funciones.

Saberes estructurantes de la unidad curricular:

1. Autenticación:

    a) Principios de autenticación de usuario.

    b) Autenticación de usuarios basada en secretos y en tokens.

    c) Mecanismos biométricos.

    d) Autenticación remota

2. Control de acceso:

    a) Principios de control de acceso.

    b) Sujetos, objetos y permisos.

    c) Control de acceso discrecional (DAC).

    d) Control de acceso basado en roles (RBAC).

    e) Control de acceso basado en atributos (ABAC).

    f) Gestión de identidades, credenciales y de acceso

3. Seguridad de Sistemas Operativos:

    a) Planificación de la seguridad de SO y Hardening.

    b) Mantenimiento: Logging y Backup.

    c) Seguridad Linux/Unix.

    d) Seguridad Windows.

    e) Seguridad de sistemas de virtualización.

4. Computación confiable y Seguridad Multinivel:

    a) El modelo Bell-LaPadula para seguridad computacional.

    b) Otros modelos.

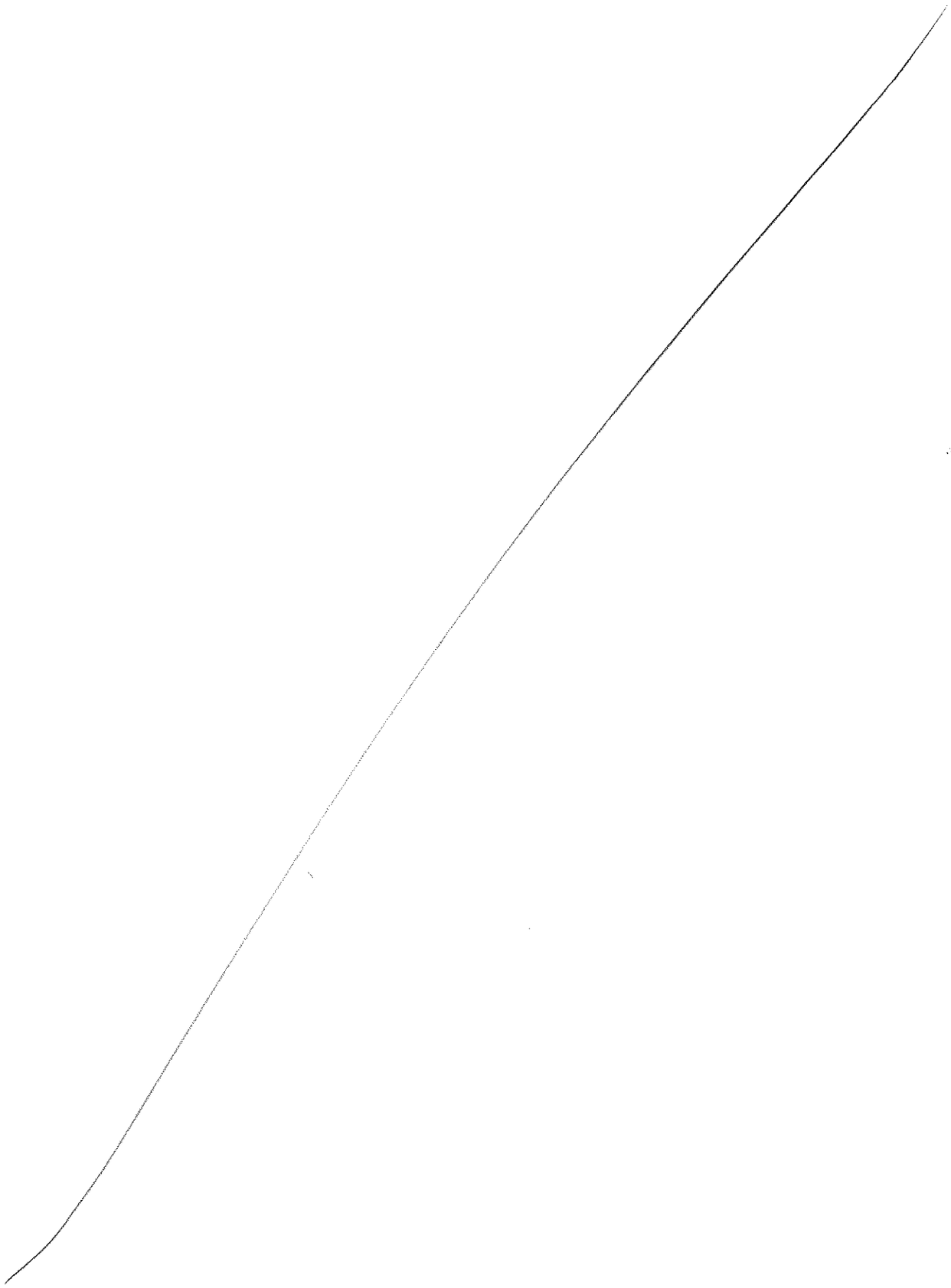
    c) El concepto de modelo confiable.

    d) Aplicaciones de seguridad multinivel.

Bibliografía Básica

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

Gollman, Dieter (2009), Computer Security, Wiley Computing Publishing, 3rd. Editon.



32

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		2			
SEMESTRE/ MÓDULO		3			
UNIDAD CURRICULAR		Criptografía aplicada			
CRÉDITO EDUCATIVO		13			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 8		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

El objetivo de esta unidad curricular es que el estudiante conozca los fundamentos matemáticos de la criptografía, las principales primitivas criptográficas, identifique conceptos y propiedades fundamentales de la criptografía aplicada así como algunas malas prácticas que las hacen vulnerables en el uso.

Resultados de aprendizaje:

- Explica el funcionamiento básico de los algoritmos de cifrado de bloques simétricos.
- Compara y contrasta el cifrado de bloques y el cifrado de secuencias.
- Discute el uso de funciones hash seguras para la autenticación de mensajes.
- Lista otras aplicaciones de funciones hash seguras.
- Explica el funcionamiento básico de los algoritmos de cifrado de bloques asimétricos.
- Presenta una descripción general del mecanismo de firma digital y explica el concepto de sobres digitales.
- Explica la importancia de los números aleatorios y pseudoaleatorios en criptografía.

Saberes estructurantes de la unidad curricular:

1. Confidencialidad con cifrado simétrico:
a) Cifrado simétrico.
b) Algoritmos de cifrado de bloques simétricos.
c) Cifrados de flujo.

2. Autenticación de mensajes y funciones hash:
a) Autenticación mediante cifrado simétrico.
b) Autenticación de mensajes sin cifrado de mensajes.
c) Funciones hash seguras.
d) Otras aplicaciones de las funciones hash.

3. Cifrado de clave pública:
a) Estructura de cifrado de clave pública.
b) Aplicaciones para criptosistemas de clave pública.
c) Requisitos para criptografía de clave pública.

d) Algoritmos de cifrado asimétrico.

4. Firmas digitales y gestión de claves:

a) Firma digital.

b) Certificados de clave pública.

c) Intercambio de claves simétricas utilizando cifrado de clave pública.

d) Sobres digitales.

5. Números aleatorios y seudoaleatorios:

a) El uso de números aleatorios.

b) Aleatorio versus pseudoaleatorio.

Bibliografía

Básica

W. Stallings; Criptography and Network Security, Prentice Hall, (2006).

Complementaria

1. W. Stallings, L. Brown; Computer Security: Principles and Practice, Pearson, 4th Edition, (2018). 2. R. Anderson; Security Engineering: A Guide to Building Dependable Distributed Systems, Ed. Wiley, 3rd. Edition, (2020).

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		2			
SEMESTRE/ MÓDULO		4			
ASIGNATURA			Taller de programación segura		
CRÉDITO EDUCATIVO		13			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 8		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

El objetivo de esta unidad curricular es introducir técnicas y herramientas, metodológicas y tecnológicas, para la verificación de seguridad de aplicaciones. El taller consta de dos módulos donde se ejercitan prácticas ofensivas y defensivas respectivamente. Se pretende mediante actividades prácticas que los estudiantes incorporen los conocimientos para la ejecución de análisis de seguridad o test de penetración, así como aprender a utilizar herramientas y tecnologías de seguridad para la identificación de vulnerabildades durante el desarrollo y despliegue de aplicaciones.

Saberes estructurantes de la unidad curricular:

1) Práctica ofensiva

- Objetivo: uso de métodos y herramientas para la aplicación de tests de penetración y similares propios del enfoque DAST (Dynamic Application Security Testing).
- Ejemplo de herramientas: OWASP ZAP, Burp Suite, Greenbone OpenVAS.

2) Práctica defensiva

- Objetivo: se pondrá foco en prácticas que permiten aplicar controles a lo largo de todo el ciclo de desarrollo, en particular para realizar verificaciones tanto con el enfoque DAST como con el enfoque SAST (Static Application Security Testing).
- Ejemplo de herramientas: OWASP ZAP, Sonarqube, OWASP Dependency Check, Kube Hunter, Kube Benc

Bibliografía

Básica

D. Fisher, Application Security Program Handbook, 2022.

L. Bell, M. Brunton-Spall, R. Smith, J. Bird, Application Security:
Enabling Security in a Continuous Delivery Pipeline, 2017.

Complementaria

OWASP WSTG, https://owasp.org/www-project-web-security-testingguide/.

OWASP Top 10, https://owasp.org/www-project-top-ten/.

SANS Top 25 software errors, https://www.sans.org/top25-softwareerrors/

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		2			
SEMESTRE/ MÓDULO		4			
UNIDAD CURRICULAR		Seguridad en Redes de Computadoras			
CRÉDITO EDUCATIVO		13			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 8		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

El objetivo de este curso es introducir al estudiante en los conceptos básicos de la seguridad informática de redes de datos TCP/IP.

Resultados de aprendizajes:

Incorpora conceptos básicos necesarios para identificar las posibles amenazas que puede sufrir una red de datos TCP/IP

Establece los mecanismos de protección adecuados.

Saberes estructurantes de la unidad curricular:

1. Problemas de Seguridad de los protocolos TCP/IP
    a) Autenticación del origen (IP spoofing).
    b) Interacción IP/MAC, ARP spoofing.
    c) Ataques a protocolo de ruteo, ICMP.
    d) TCP session Hijacking, SYN Flooding.
    e) Capa de Aplicación: Servicio DNS.
    f) VLAN
2. Redes inalámbricas (WiFi):
    a) Requerimientos de seguridad (autenticación, control de acceso, confidencialidad, integridad).
    b) WEP, WPA, WPA2, EAP, 802.1X
3. Seguridad IP (IPSec):
    a) Asociaciones de Seguridad (SA).
    b) Modos de funcionamiento (túnel y transporte).
    c) Protocolo AH y ESP (encabezados y servicios que ofrecen).
    d) IPSec Key Management (IKE).
    e) IPsec y filtrado.
4. VPN
    a) ¿Qué es una VPN? VPN sobre Internet.
    b) Implementación de VPN.
5. Firewalls
    a) Definición. ¿Qué puede hacer y qué NO un firewall?.
    b) Filtrado de paquetes, con y sin estados. Generando reglas de filtrado.

c) Logging.

d) Arquitecturas de Firewall.

e) Tipos de Firewall.

f) Servicios Proxy y NAT.

6. Sistemas de detección y prevención de intrusiones (IDS/IPS):

a) Definición.

b) Clasificación y formas de detección.

c) Falsos positivos y negativos.

d) ¿Acciones automáticas? Dónde monitorizar (sensar).

e) Otro tipo de sensores (honeypots).

7. Diseño de un perímetro seguro:

a) Identificación de activos a proteger.

b) Identificación de fronteras.

c) Separación e identificación de zonas de seguridad.

Bibliografía:

Básica:

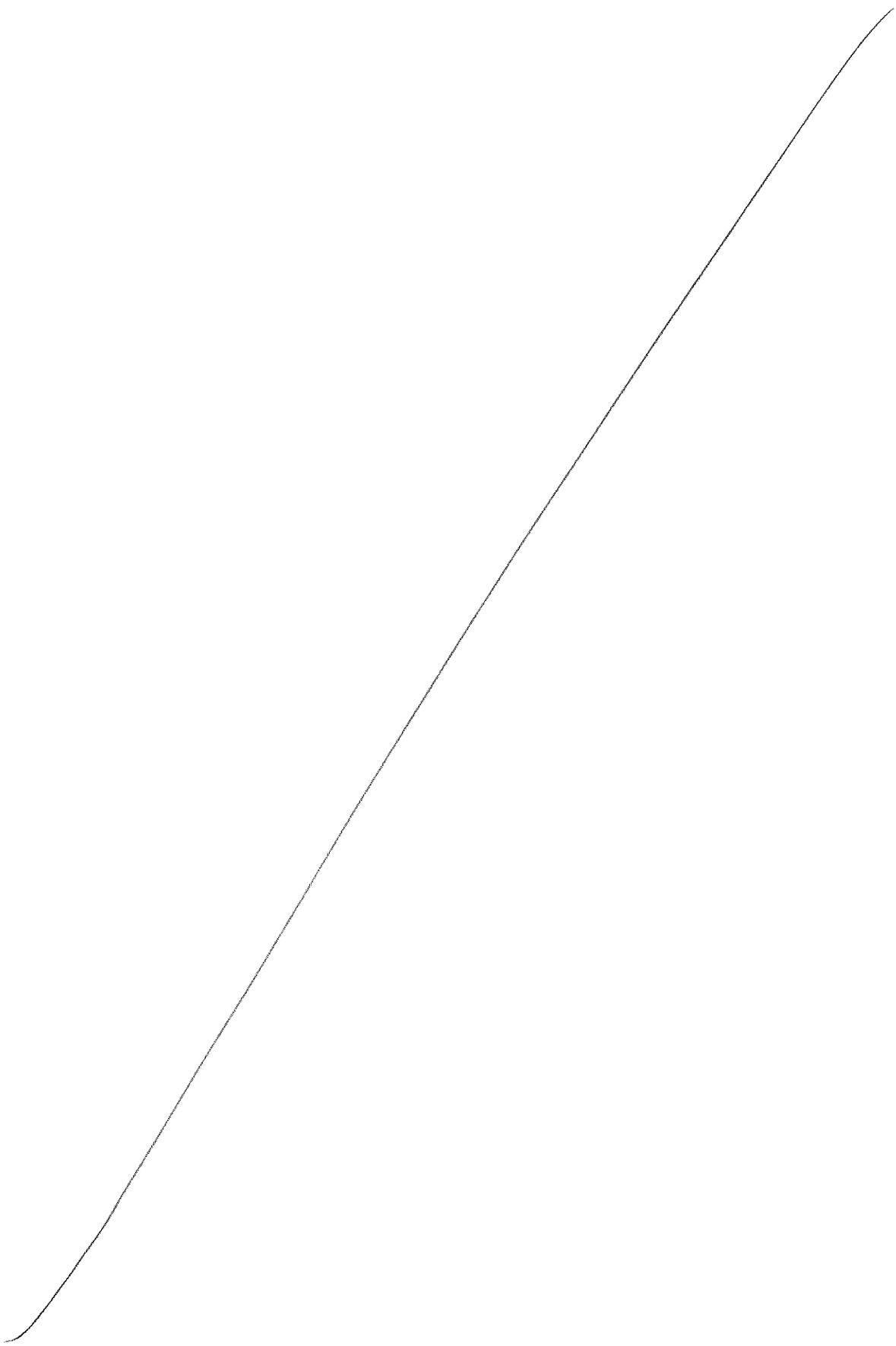
Gollman, Dieter (2009), Computer Security, Wiley Computing Publishing, 3rd. Editon.

Complementaria:

Garfinkel, S.; Spafford, G. & Schuartz, A. (2003); Practical Unix & Internet Security; Ed. O'Reilly; 3rd Edition.

Edney, J.; Arbaugh, W. (2004); Real 802.11 Security - Wi-Fi Protected Access and 802.11i. Addison-Wesley, 2004.

Zwicky, E.; Cooper, S. & Chapman, B. (2000); Building Internet Firewalls; Ed. O'Reilly; 2nd Editon



37

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

<table>
<tr><td colspan="2"></td><td colspan="4">PROGRAMA</td></tr>
<tr><td colspan="2"></td><td>Código en SIPE</td><td colspan="3">Descripción en SIPE</td></tr>
<tr><td colspan="2">TIPO DE CURSO</td><td>028</td><td colspan="3">Tecnólogo</td></tr>
<tr><td colspan="2">PLAN</td><td colspan="4">2023</td></tr>
<tr><td colspan="2">ORIENTACIÓN</td><td>88F</td><td colspan="3">Ciberseguridad</td></tr>
<tr><td colspan="2">MODALIDAD</td><td colspan="4">Presencial</td></tr>
<tr><td colspan="2">AÑO</td><td colspan="4">2</td></tr>
<tr><td colspan="2">SEMESTRE/ MÓDULO</td><td colspan="4">4</td></tr>
<tr><td colspan="2">UNIDAD CURRICULAR</td><td></td><td colspan="3">Taller de Técnicas y Procedimientos</td></tr>
<tr><td colspan="2">CRÉDITO EDUCATIVO</td><td colspan="4">6</td></tr>
<tr><td colspan="2">DURACIÓN DEL CURSO</td><td>Horas totales: 96</td><td colspan="2">Horas semanales: 4</td><td>Cantidad de semanas: 16</td></tr>
<tr><td>Fecha de Presentación: 6/3/2023</td><td>N° Resolución de la DGETP</td><td>Exp. N°</td><td>Res. N°</td><td>Acta N°</td><td>Fecha __/__/____</td></tr>
</table>

Objetivos

El Taller de Técnicas y procedimientos es un curso fundamentalmente práctico, basado en el uso de tecnologías sobre las cuales se realizan diferentes laboratorios. En dichos laboratorios los estudiantes pueden aprender y profundizar sobre el uso de herramientas específicas de seguridad. El objetivo principal es llevar a la práctica conceptos básicos de seguridad computacional En el transcurso del Taller, se implementan servicios y funcionalidades de seguridad, que en general son menospreciados frente a aspectos funcionales del desarrollo de software tradicional, por ejemplo, desarrollando funciones de autenticación, plugins para herramientas de seguridad, modificando y configurando funcionalidades complejas de los sistemas operativos, utilización de criptografía en los canales de comunicación, entre otros. Este taller representa un complemento esencial a los conceptos teórico/práctico que son introducidos en los distintos cursos del área de formación Seguridad Computacional, aportando además una visión fuertemente focalizada en el uso de métodos técnicos empleados en el sector profesional, convirtiéndose así en un área de especialización cada vez más requerida por diferentes tipos de organizaciones.

Metodología de enseñanza

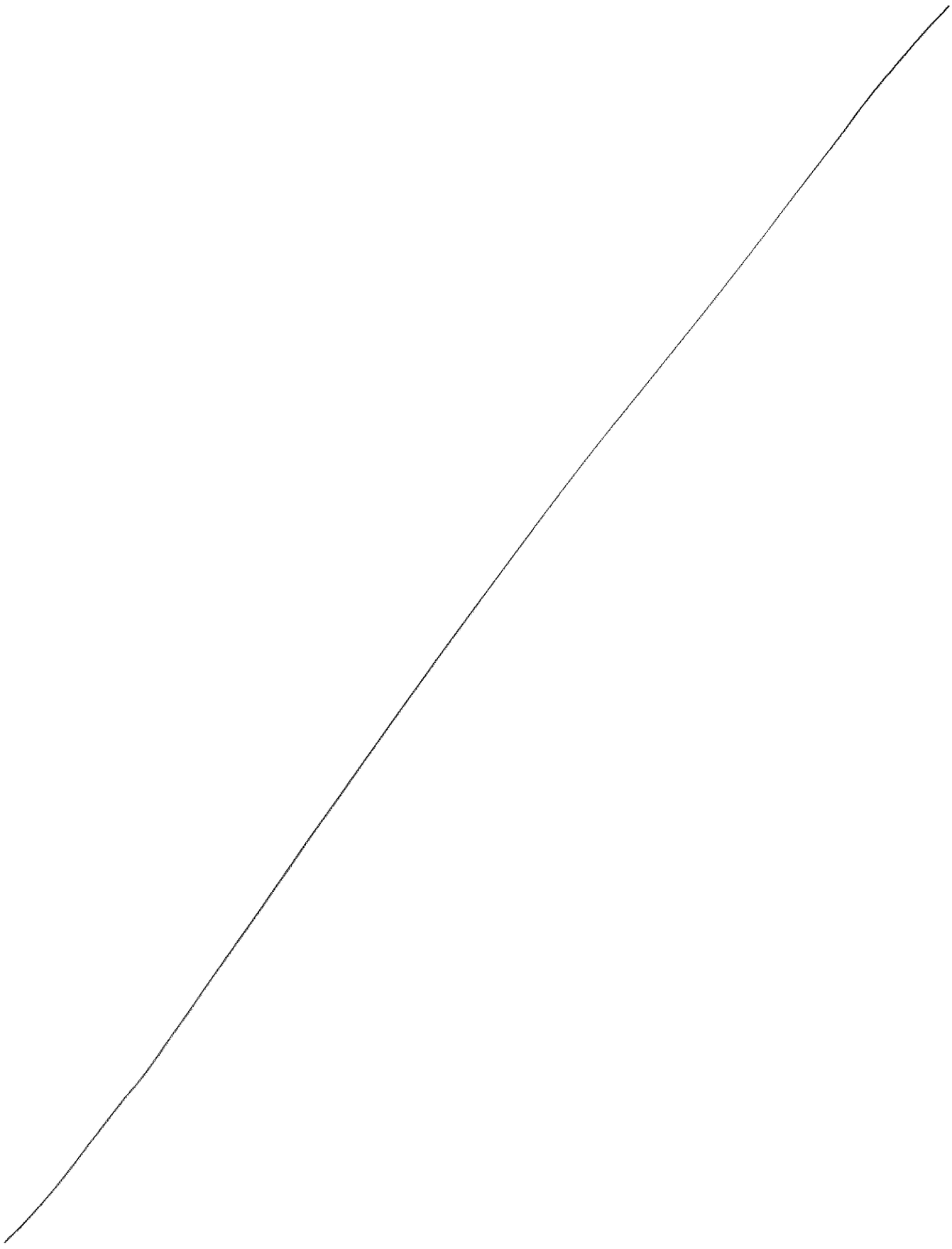
La metodología de enseñanza utilizada es la de aprendizaje basado en problemas, donde se presenta una situación que los participantes, en forma individual o grupal, deberán resolver. Se utilizan casos de la vida real, los cuales se deberán estudiar para luego proponer soluciones utilizando diferentes herramientas. Durante el transcurso de cada laboratorio se realizan distintas tareas, desde la definición del ambiente de trabajo, por ejemplo utilizando maquinas y escenarios virtuales, hasta la implementación de soluciones utilizando librerías de seguridad de diferentes lenguajes de programación. Además se pueden utilizar técnicas de juegos de roles, con el objetivo de ampliar la experiencia de los estudiantes y la habilidad para resolver problemas de la vida real. Dada la modalidad del curso, se requiere un constante y cercano seguimiento por parte de los docentes en cuanto a las soluciones a implementar, ya que las mismas varían entre los diferentes grupos de estudiantes. Es necesario mantener acotado el alcance de cada tarea, sin descuidar el cumplimiento de los requerimientos básicos de cada laboratorio.

El temario de base para este taller lo constituye los conceptos fundamentales de criptografía aplicada, seguridad de sistemas operativos y de redes, y los principios de desarrollo de código

seguro. Los trabajos prácticos o laboratorios podrán varias en diferentes ediciones del taller, pero el objetivo es cubrir aspectos ingenieriles de cada unas de las mencionadas áreas.

Bibliografía

La bibliografía será especificada en cada laboratorio, para guíar al estudiante en la temática objetivo cubierta y en el uso de las herramientas necesarias para el desarrollo de los mismos.



39

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		2			
SEMESTRE/ MÓDULO		4			
ASIGNATURA		Gestión de la Seguridad de la Información			
CRÉDITO EDUCATIVO		13			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 8		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

Introducir a los estudiantes en los principales conceptos y metodologías asociadas a la gestión de la ciberseguridad, contemplando el marco normativo internacional y nacional existente. Llevar a la práctica una metodología de rápida aplicación para la implementación de un Sistema de Gestión de Seguridad de la Información. Presentar metodologías y buenas prácticas concretas para la gestión de riesgos, gestión de incidentes, gestión de la continuidad de la seguridad y gestión de vulnerabilidades. Se abarcarán las principales conceptos entorno a la familia de normas ISO/IEC 27000 y el marco de ciberseguridad de NIST.

Saberes estructurantes de la unidad curricular:

1. Introducción:
    a) Definiciones y conceptos de gestión de ciberseguridad.
    b) Confidencialidad, Integridad y Disponibilidad.
    c) Marco normativo nacional e internacional.
2. Sistema de Gestión de Seguridad de la Información:
    a) Metodologías de implantación.
    b) Principales desafíos a enfrentar.
    c) Herramientas disponibles que faciliten la implantación.
3. Gestión de Riesgos:
    a) Introducción al proceso de gestión de riesgos.
    b) Metodologías de análisis de riesgo.
    c) Tratamiento de riesgos.
4. Gestión de incidentes:
    a) Definición de incidentes.
    b) Procesos de clasificación, análisis, tratamiento, resolución y cierre.
    c) Control de flujos de información y procesos.
    d) Modelos organizacionales de Centros de Respuesta y Centros Operativos de Seguridad
5. Gestión de la continuidad operativa:
    a) Componentes del negocio.
    b) Tipos de desastres que deben considerarse.c
    c) Análisis de Impacto del Negocio.
    d) Desarrollo de estrategias de mitigación.

40

Bibliografía:

H. Tipton, M. Krause, Information Security Management Handbook 6th, 2008.

Thomas Peltier, Information Security Policies, Procedures and Standards, 2002.

L. Hayden, IT Security Metrics. A Practical Framework for Measuring Security and Protecting Data, 2010.

Proyecto AMPARO, Manual básico de Gestión de Incidentes de Seguridad Informática, 2012.

Susan Snedaker, Business Continuity and Disaster Recovery for IT professionals, 2007.

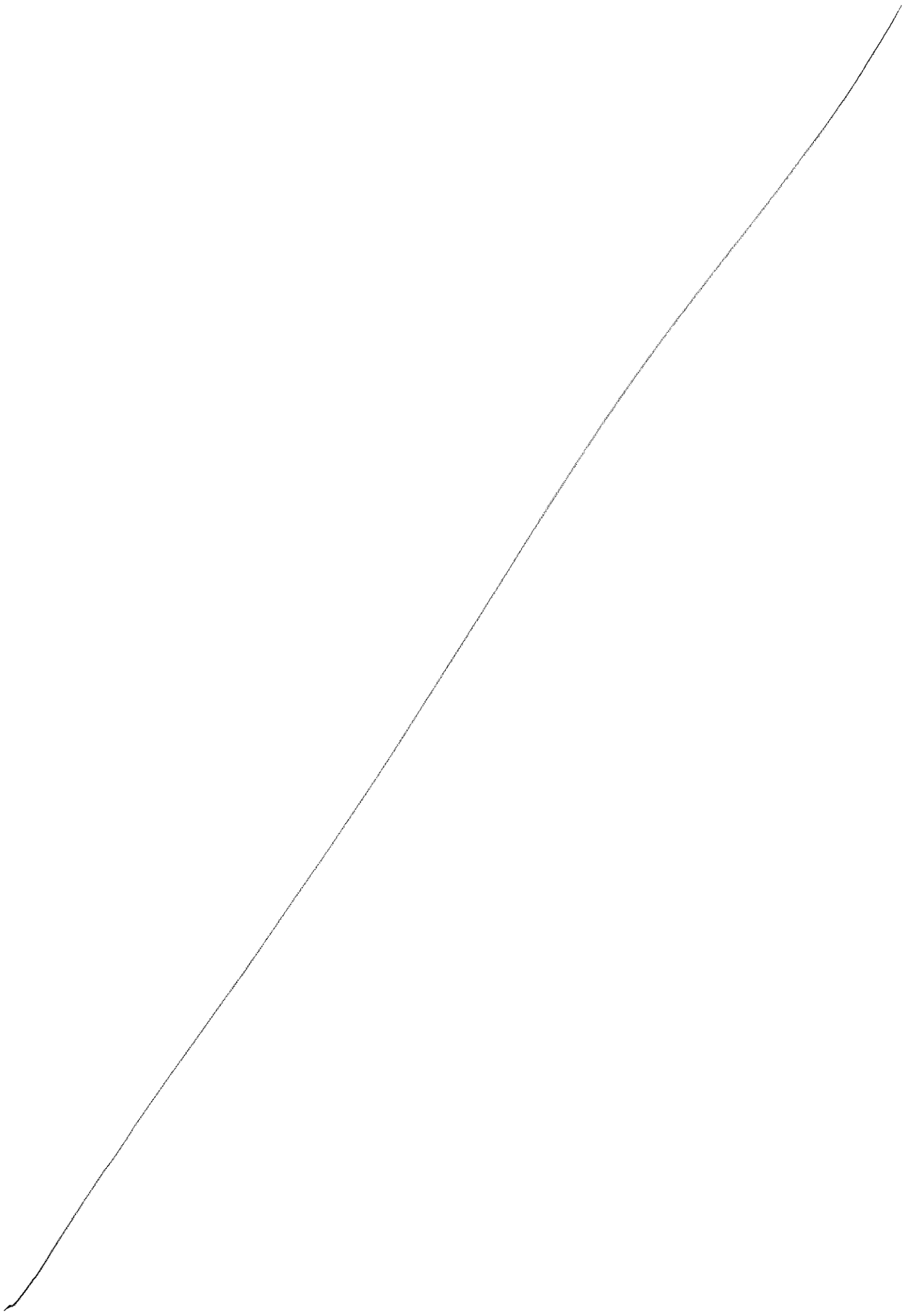
Complementaria:

NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018.

AGESIC, Marco de Ciberseguridad, 2019.

H. Allen et al, Structuring the Chief Information Security Officer Organization, CERT Division, Software Engineering Institute, Carnegie Mellon University.

C. Zimmerman, Ten Strategies of a World-Class Cybersecurity Operations Center, MITRE Corporation.



41

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		3			
SEMESTRE/ MÓDULO		5-6			
UNIDAD CURRICULAR		Configuración y Administración segura de sistema Electiva			
CRÉDITO EDUCATIVO		11			
DURACIÓN DEL CURSO		Horas totales: 112	Horas semanales: 7		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivos:

La administración de sistemas se encarga de garantizar la correcta, ininterrumpida y segura operación de los equipos, redes y servicios de una infraestructura de un nivel de complejidad relativamente alto. Las tareas que suelen incluirse en esta disciplina pueden ser: instalación y configuración de sistemas de hardware y software (tanto en instalaciones propias de las organización como en la nube); administración de redes; monitoreo de la infraestructura; diagnóstico y solución de problemas; respuesta a incidentes y recuperación ante fallas; auditorías; etc. Esta actividad curricular profundiza los conocimientos de sistemas operativos, redes y seguridad computacional vistos a lo largo de la carrera, brindándole a los estudiantes capacidades de alto nivel y una visión más global del rol del administrador de sistemas con un foco en operación segura de las infraestructuras.

Resultados de aprendizajes:

- Concibe el rol de un administrador de sistemas en una organización.
- Conoce la administración de equipos de hardware, como su adquisición, mantenimiento y aseguramiento físico.
- Realiza el hardening de sistemas operativos. Conocer diferentes arquitecturas de red y sus efectos en la ciberseguridad.
- Maneja tecnologías de virtualización y ser capaz de desplegar servicios en la nube.
- Domina técnicas y herramientas que garantizan alta disponibilidad.
- Monta sistemas de monitoreo y alerta de la infraestructura.
- Responde frente a fallas o incidentes de seguridad, de modo de garantizar la continuidad del negocio.
- Integra la ciberseguridad como un aspecto fundamental del correcto mantenimiento y operación de los sistemas de una organización.

Saberes estructurantes de la unidad curricular:

1. Fundamentos de la administración de sistemas
    a) Motivación, cometidos y tareas de la administración de sistemas.
    b) Consideraciones éticas de la disciplina.
    c) Privacidad y protección de datos personales en la administración de sistemas.
2. Infraestructura física:
    a) Adquisición, instalación y mantenimiento de hardware.

b) Sistemas de inventario.

c) Seguridad física.

3. Administración de Sistemas Operativos:

a) Políticas de gestión de usuarios.

b) Servicios de directorio.

c) Hardening.

4. Administración de Redes:

a) Arquitecturas seguras de redes.

b) Segmentación e identificación de zonas de seguridad.

c) Defensa en profundidad.

d) Redes definidas por software, micro-segmentación, arquitecturas zero trust.

5. Virtualización y nube:

a) Tecnologías de virtualización y containers.

b) Cloud computing.

c) Infrastructure as Code y DevOps.

6. Alta disponibilidad y tolerancia a fallos:

a) Mecanismos y herramientas de redundancia.

b) Diseño y gestión de respaldos.

7. Diagnóstico y resolución de problemas:

a) Monitoreo y sistemas de alerta.

b) Auditoría, logging y gestión de eventos e información de seguridad (SIEMs).

c) Respuesta ante fallas e incidentes de seguridad.

Bibliografía

Básica:

J. Davis; Modern System Administration; 1st Edition (2022).

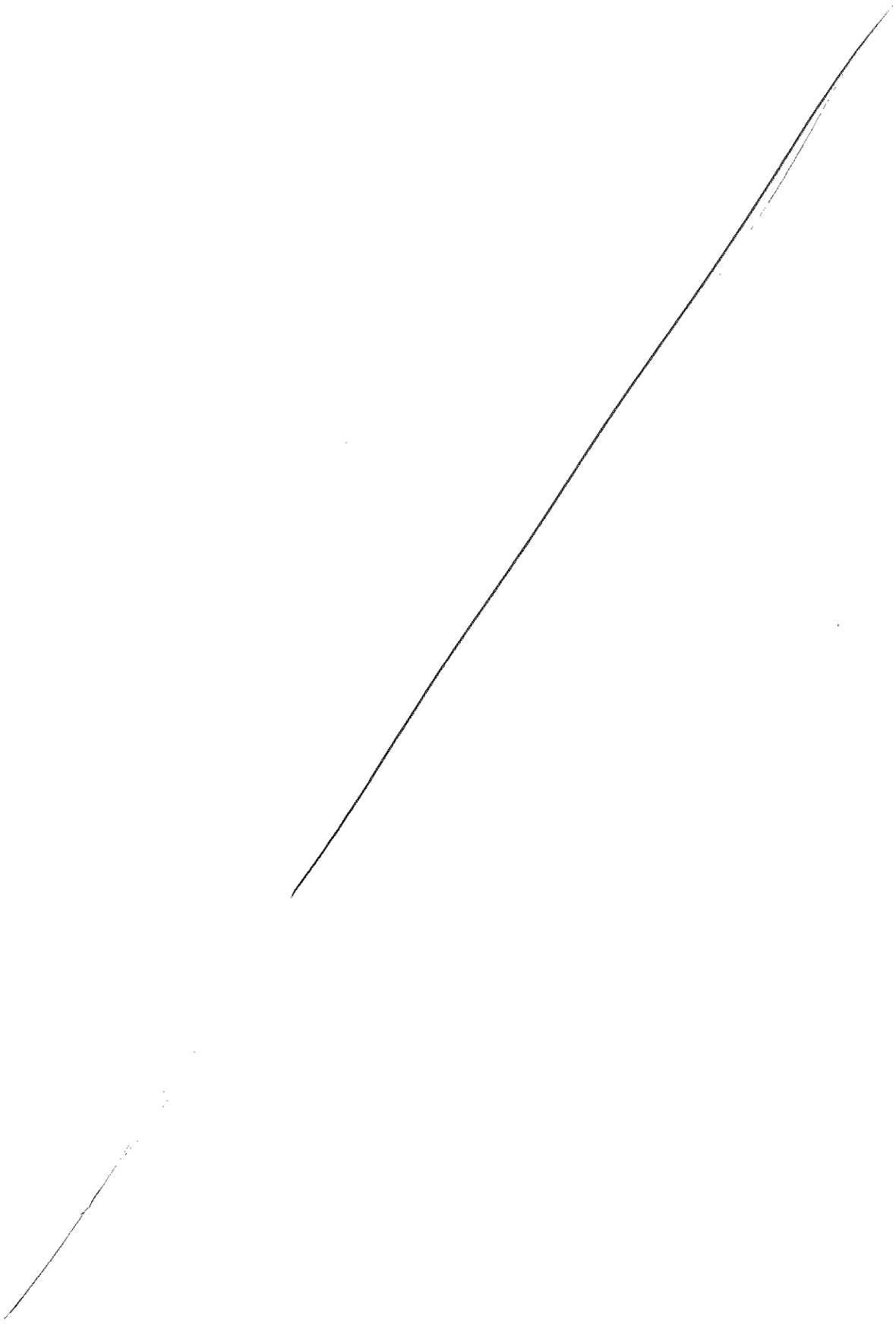
Complementaria:

T. Hein, E. Nemeth, G. Snyder, B. Whaley, D. Mackin; UNIX and Linux System Administration Handbook; 5th Edition (2017).

B. Dauti; Windows Server 2022 Administration Fundamentals; 3rd Edition (2022).

M. Julian; Practical Monitoring: Effective Strategies for the Real World; 1st Edition (2017).

G. Kim, P. Debois, J. Willis, J. Humble; The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations; 2nd Edition (2021)



43

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		3			
SEMESTRE/ MÓDULO		5-6			
UNIDAD CURRICULAR			Introducción al Análisis Forense Digital Electiva		
CRÉDITO EDUCATIVO		11			
DURACIÓN DEL CURSO		Horas totales: 112	Horas semanales: 7		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	N° Resolución de la DGETP	Exp. N°	Res. N°	Acta N°	Fecha __/__/____

Objetivo:

El objetivo de esta unidad curricular es introducir al estudiante en los conceptos básicos del análisis forense informático.

Al finalizar el curso el alumno habrá adquirido los conceptos técnicos básicos necesarios en lo que respecta a las metodologías de análisis y el tratamiento y/o adquisición de la evidencia digital.

Saberes estructurantes de la unidad curricular:

1. Bases y Motivación:
    a) Introducción.
    b) Motivación, definiciones y objetivos del análisis forense informático.
    c) Principios y usos del análisis informático forense.
2. Evidencia digital:
    a) Tipos de evidencia.
    b) Propiedades.
    c) Fuentes de obtención de evidencias.
    d) Cadena de custodia.
3. Tipos de análisis forense:
    a) Análisis post-mortem.
    b) Live análisis.
    c) Análisis On-Sitey en el laboratorio
4. Metodologías para el análisis forense digital:
    a) Identificación.
    b) Preservación.
    c) Análisis.
    d) Presentación.
    e) Herramientas de soporte a la metodología.
5. Anti-forensia:
    a) Problemáticas y desafíos del análisis forense informático.
    b) Técnicas anti-forenses.
    c) Clasificación de métodos anti-forenses.
    d) Herramientas anti-forenses.

Bibliografía:

Básica:

Joakim Kävrestad, Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications, Springer London, 2nd Edition, (2020).

Complementaria:

Eoghan Casey (Editor), Handbook of Digital Forensics and Investigation, Elsevier, 1st Edition, (2010).