1. DATOS INFORMATIVOS

DOMINIO:			
CARRERA: Ingeniería en Ciberseguridad y Gestión de Tecnologías de la Información			
Asignatura/Módulo: Programación IV			
Paralelo:			**N° horas**
Plan de estudios:			H. aprendizaje en contacto con el docente: 32
Prerrequisitos: Programación II y Planteamiento de			
Periodo académico: 2026-01			H. aprendizaje autónomo: 72
			H. aprendizaje práctico-experimental: 16
Docenteo o Co-Docente 1:	**Grado académico y título profesional:**	**Co-Docente 2:**	**Grado académico y título profesional:**
Damián Nicolalde	Máster en redes de comunicaciones, MBA		
Breve reseña de la actividad académica y/o profesional:		**Breve reseña de la actividad académica y/o**	
Damián Anibal Nicolalde Rodríguez es profesor e investigador en la Facultad de Ingeniería de la Pontificia Universidad Católica del Ecuador (PUCE). Su trabajo se centra en áreas como redes inalámbricas, eficiencia energética, redes de sensores inalámbricos, redes neuronales y analítica de aprendizaje. Ha participado en varios proyectos de investigación, incluyendo la evaluación del rendimiento del protocolo TCP/IP en redes satelitales de órbita baja y el desarrollo de prototipos de antenas reconfigurables para redes celulares. Además, su investigación contribuye a los Objetivos de Desarrollo Sostenible de las Naciones Unidas.			
Indicación de horario de atención al estudiante:			
Tutoría presencial:		**Teléfono:**	2991700 ext 1154
Tutoría virtual:		**Correo electrónico:**	nombre@puce.edu.ec

2. DESCRIPCIÓN DE LA ASIGNATURA

La asignatura Programación IV – Estructuras de Datos II tiene como propósito profundizar en el análisis, implementación y selección estratégica de algoritmos y estructuras de datos avanzadas, orientadas a la resolución de problemas de complejidad media y alta en contextos de ciberseguridad. A través del estudio de algoritmos de búsqueda y ordenamiento, árboles y grafos, el estudiante desarrolla competencias para evaluar la eficiencia computacional, modelar información estructurada y no estructurada, y tomar decisiones técnicas fundamentadas sobre la estructura de datos más adecuada según el problema planteado. La asignatura se desarrolla bajo una metodología de Aprendizaje Basado en Proyectos y Retos (ABP-R), donde los estudiantes construyen progresivamente un sistema de análisis de incidentes de seguridad, integrando teoría, práctica y justificación ingenieril, fortaleciendo así su capacidad de diseño de soluciones robustas, eficientes y alineadas con escenarios reales de la disciplina.

3. DESCRIPCIÓN DE COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

COMPETENCIAS TRANSVERSALES	COMPETENCIAS DISCIPLINARES DEL DOMINIO	RESULTADOS DE APRENDIZAJE DE LA CARRERA	RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA
		Aplicar los principios de programación para el diseño e implementación de soluciones de software eficientes y escalables, cumpliendo con los estándares de calidad y seguridad.	Comprender los conceptos de algoritmos y estructuras de datos, analizando su funcionamiento y eficiencia computacional en la resolución de problemas de ciberseguridad.
		Aplicar los principios de programación para el diseño e implementación de soluciones de software eficientes y escalables, cumpliendo con los estándares de calidad y seguridad.	Desarrollar algoritmos y estructuras de datos avanzadas para la resolución de problemas de complejidad media-alta, considerando criterios de eficiencia computacional en escenarios de ciberseguridad.
		Implementar algoritmos y estructuras de datos para la resolución de problemas de complejidad media y alta en distintas áreas de la computación.	Seleccionar las estructuras de datos más adecuadas según los requerimientos y características de distintos escenarios de ciberseguridad.

4. EVALUACIÓN DE LOGROS DE APRENDIZAJE

PROYECTO DEL NIVEL	Retos	Resultado de aprendizaje	Pesos	Definición del criterio de evaluación del RdA	Ponderación criterios	Nivel de logro alcanzado al RdA				Observaciones (Alertas para tutorías académicas)
						Alcanzado con excelencia (A) (45-50)	Alcanzado muy bueno (B) (40-44)	Alcanzado bueno (C) (30-39)	Pendiente de alcanzar (D) (29 y menos)	
Sistema de Análisis y Modelado de Incidentes de Ciberseguridad El proyecto de la asignatura consiste en el diseño y desarrollo incremental de un sistema de Análisis y Modelado de Incidentes de Ciberseguridad, cuyo objetivo es organizar, procesar y analizar información relacionada con eventos de seguridad mediante el uso de algoritmos de búsqueda, algoritmos de ordenamiento, árboles y grafos. A lo largo del semestre, el estudiante trabajará sobre un mismo sistema, incorporando de manera incremental los contenidos abordados en cada bloque temático, hasta consolidar una solución integrada que permita modelar escenarios reales de ciberseguridad, como el análisis de logs, la evaluación de rutas de ataque, la identificación de nodos críticos o la optimización del procesamiento de eventos. El proyecto se desarrolla bajo la metodología de Aprendizaje Basado en Proyectos y Retos (ABPR) y está estructurado en cuatro retos: tres de carácter formativo y un reto final de carácter sumativo. Cada reto constituye un entregable parcial que fortalece progresivamente el sistema, permitiendo al estudiante aplicar los conceptos aprendidos, analizar la eficiencia de sus soluciones y justificar técnicamente la selección de las estructuras de datos empleadas.	RETO 1 – Análisis algorítmico de eventos de seguridad (Reto formativo) En este primer reto, el estudiante se enfoca en la comprensión y análisis de algoritmos, aplicados al procesamiento de datos asociados a eventos de ciberseguridad. A partir de conjuntos de datos simulados (por ejemplo, registros de accesos, direcciones IP, usuarios o eventos), el estudiante implementa y compara algoritmos de búsqueda y de ordenamiento, evaluando su comportamiento y eficiencia. El propósito de este reto es que el estudiante comprenda cómo la elección de un algoritmo impacta directamente en el rendimiento de un sistema de seguridad, sentando las bases conceptuales para la toma de decisiones técnicas en los retos posteriores.	Comprender los conceptos de algoritmos y estructuras de datos, analizando su funcionamiento y eficiencia computacional en la resolución de problemas de ciberseguridad.	33.33	Criterio 1: Comprende los principios de los algoritmos de búsqueda y ordenamiento, identificando su funcionamiento y complejidad temporal y espacial en escenarios de ciberseguridad.	50%	Comprende de manera integral los algoritmos y estructuras de datos, explicando con precisión su funcionamiento, complejidad y comportamiento en distintos escenarios de eventos de seguridad.	Comprende adecuadamente los algoritmos y estructuras de datos, identificando su funcionamiento y complejidad con ligeras imprecisiones conceptuales.	Comprende parcialmente los algoritmos y estructuras de datos, con explicaciones generales y limitaciones en el análisis de complejidad.	No logra comprender los conceptos fundamentales de algoritmos y estructuras de datos, presentando errores conceptuales significativos.	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.
				Criterio 2: Comprende el impacto de la elección de algoritmos en el rendimiento de un sistema de análisis de incidentes de ciberseguridad.	50%	Comprende claramente cómo la selección algorítmica impacta en el rendimiento del sistema, justificando sus análisis con ejemplos y evidencias experimentales.	Comprende el impacto del algoritmo en el rendimiento del sistema, aunque con análisis menos profundos o ejemplos limitados.	Comprende de forma básica el impacto del algoritmo en el rendimiento, con justificaciones superficiales.	No comprende la relación entre la selección algorítmica y el rendimiento del sistema.	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.
	RETO 2 – Optimización del procesamiento y organización de la información (Reto formativo) En el segundo reto, el estudiante profundiza en la implementación de algoritmos más eficientes y estructuras de datos jerárquicas, orientadas a mejorar el rendimiento del sistema. Se incorporan algoritmos de ordenamiento avanzados y árboles como mecanismos para optimizar la búsqueda y organización de información. Este reto busca que el estudiante no solo implemente soluciones funcionales, sino que analice su eficiencia computacional y reflexione sobre su aplicabilidad en escenarios donde se manejan grandes volúmenes de datos de seguridad.	Desarrollar algoritmos y estructuras de datos avanzadas para la resolución de problemas de complejidad media-alta, considerando criterios de eficiencia computacional en escenarios de ciberseguridad.	33.33	Criterio 1: Desarrolla algoritmos de ordenamiento avanzados y estructuras jerárquicas para optimizar el procesamiento de información de seguridad.	50%	Desarrolla correctamente algoritmos y estructuras avanzadas, logrando soluciones eficientes, funcionales y optimizadas para grandes volúmenes de datos.	Desarrolla algoritmos y estructuras avanzadas de forma funcional, con pequeñas oportunidades de mejora en eficiencia.	Desarrolla algoritmos avanzados de manera parcial o con limitaciones en su eficiencia.	No logra desarrollar algoritmos o estructuras avanzadas de forma funcional.	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.
				Criterio 2: Desarrolla soluciones algorítmicas considerando criterios de eficiencia computacional en escenarios de ciberseguridad.	50%	Desarrolla soluciones altamente eficientes, justificando decisiones técnicas basadas en complejidad y rendimiento.	Desarrolla soluciones eficientes con justificación técnica adecuada, aunque no completamente optimizada.	Desarrolla soluciones funcionales con análisis limitado de eficiencia.	No considera criterios de eficiencia en el desarrollo de las soluciones.	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.
	RETO 3 – Modelado estructural de escenarios de ciberseguridad (Reto formativo) El tercer reto se centra en el modelado estructural de la información, utilizando árboles y grafos para representar relaciones, dependencias y flujos dentro de un escenario de ciberseguridad. El estudiante emplea estas estructuras para modelar infraestructuras de red, rutas de ataque, relaciones entre eventos o dependencias entre componentes críticos. En este punto, el estudiante comienza a seleccionar y justificar las estructuras de datos más adecuadas según el problema planteado, integrando análisis conceptual y técnico.	Seleccionar las estructuras de datos más adecuadas según los requerimientos y características de distintos escenarios de ciberseguridad.	33.34	Criterio 1: Selecciona estructuras de datos adecuadas (árboles y grafos) para modelar escenarios de ciberseguridad.	50%	Selecciona de forma precisa y justificada las estructuras de datos más adecuadas para el problema planteado.	Selecciona estructuras de datos apropiadas, con justificación técnica aceptable.	Selecciona estructuras de datos funcionales, con justificación limitada.	No selecciona estructuras de datos adecuadas para el problema planteado.	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.
	RETO 4 – Sistema integrado de análisis de ciberseguridad (Reto sumativo – Proyecto final) El reto final corresponde a la integración completa del sistema, consolidando los aprendizajes desarrollados a lo largo de la asignatura. El estudiante integra algoritmos de búsqueda, algoritmos de ordenamiento, árboles y grafos en una solución funcional orientada a un escenario realista de ciberseguridad. Este reto requiere justificar técnicamente las decisiones de diseño, analizar la eficiencia del sistema y presentar el proyecto como una solución coherente, robusta y alineada con los principios de la ingeniería y la seguridad informática. Este reto constituye la evaluación sumativa de la asignatura y evidencia el logro de los resultados de aprendizaje del nivel.			Criterio 2: Selecciona y justifica estructuras de datos considerando relaciones, dependencias y flujos en escenarios de ciberseguridad.	50%	Selecciona y justifica sólidamente las estructuras de datos considerando criterios técnicos y contextuales de seguridad.	Selecciona y justifica las estructuras con argumentos técnicos adecuados.	Selecciona estructuras con justificación básica o incompleta.	No justifica adecuadamente la selección de estructuras de datos.	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.

5. METODOLOGÍA

La asignatura se desarrolla bajo la metodología de Aprendizaje Basado en Proyectos y Retos (ABP-R), en la cual el estudiante construye de manera progresiva un proyecto que articula los contenidos teóricos y prácticos del curso. Cada bloque temático se vincula a un reto específico que orienta al estudiante a aplicar algoritmos y estructuras de datos en escenarios contextualizados de ciberseguridad, promoviendo el análisis, la experimentación y la toma de decisiones técnicas fundamentadas. La metodología combina actividades sincrónicas y asincrónicas, análisis de casos, laboratorios de programación y retroalimentación continua, con el propósito de fortalecer el razonamiento algorítmico, la eficiencia computacional y la capacidad de diseñar soluciones estructuradas, coherentes y alineadas con problemáticas reales del ámbito de la seguridad informática.

6. RELACIÓN RESULTADOS DE APRENDIZAJE, EXPERIENCIAS DE APRENDIZAJES Y DIMENSIÓN DEL CONOCIMIENTO

PROYECTO DE NIVEL	RETOS	RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA	Semanas	Experiencias / estrategias Aprendizaje en contacto con el docente	Horas	Recursos	Escenario	Experiencias / estrategias de aprendizaje práctico-experimental:	Horas	Recursos	Escenario	Experiencias / estrategias de aprendizaje autónomo	Horas	Recursos	Escenario	DIMENSIÓN DEL CONOCIMIENTO (conceptos, hecho, procedimientos o principios)
Sistema de Análisis y Modelado de Incidentes de Ciberseguridad El proyecto de la asignatura consiste en el diseño y desarrollo progresivo de un Sistema de Análisis y Modelado de Incidentes de Ciberseguridad, cuyo objetivo es organizar, procesar y analizar información relacionada con eventos de seguridad mediante el uso de algoritmos de búsqueda, algoritmos de ordenamiento, árboles y grafos. A lo largo del semestre, el estudiante trabajará sobre un mismo sistema, incorporando de manera incremental los contenidos abordados en cada bloque temático, hasta consolidar una solución integrada que permita modelar escenarios reales de ciberseguridad, como el análisis de logs, la evaluación de rutas de ataque, la identificación de nodos críticos o la optimización del procesamiento de eventos. El proyecto se desarrolla bajo la metodología de Aprendizaje Basado en Proyectos y Retos (ABP-R) y está estructurado en cuatro retos: tres de carácter formativo y un reto final de carácter sumativo. Cada reto constituye un entregable parcial que fortalece progresivamente el sistema, permitiendo al estudiante aplicar los conceptos aprendidos, analizar la eficiencia de sus soluciones y justificar técnicamente la selección de las estructuras de datos empleadas.	RETO 1 – Análisis algorítmico de eventos de seguridad (Reto formativo) En este primer reto, el estudiante se enfoca en la comprensión y análisis de algoritmos, aplicados al procesamiento de datos asociados a eventos de ciberseguridad. A partir de conjuntos de datos simulados (por ejemplo, registros de accesos, direcciones IP, usuarios o eventos), el estudiante implementa y compara algoritmos de búsqueda y de ordenamiento, evaluando su comportamiento y eficiencia. El propósito de este reto es que el estudiante comprenda cómo la elección de un algoritmo impacta directamente en el rendimiento de un sistema de seguridad, sentando las bases conceptuales para la toma de decisiones técnicas en los retos posteriores.	Comprender los conceptos de algoritmos y estructuras de datos, analizando su funcionamiento y eficiencia computacional en la resolución de problemas de ciberseguridad.	1	Tutorias sincrónicas por videoconferencia .	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante desarrolla ejercicios prácticos orientados al análisis de algoritmos, identificando su comportamiento temporal y espacial mediante ejemplos aplicados al procesamiento de eventos de seguridad. Se realizan experimentos computacionales para medir el impacto de la complejidad algorítmica en conjuntos de datos simulados.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	1. Fundamentos de algoritmos y análisis de complejidad 1.1. Concepto de algoritmo y estructura de datos 1.2. Algoritmos en la resolución de problemas de ciberseguridad 1.3. Complejidad temporal y espacial 1.4. Notación Big-O, Ω y Θ 1.5. Análisis de eficiencia en procesamiento de
			2	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante implementa y prueba algoritmos de búsqueda sobre conjuntos de datos asociados a eventos de ciberseguridad, comparando resultados y eficiencia mediante pruebas controladas. Se fomenta la experimentación para evidenciar las diferencias de rendimiento entre los métodos estudiados.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	2. Algoritmos de búsqueda 2.1. Búsqueda lineal 2.2. Búsqueda binaria 2.3. Requisitos de ordenamiento para búsqueda eficiente 2.4. Comparación de eficiencia entre métodos 2.5. Aplicaciones en búsqueda de usuarios, IPs y
			3	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante implementa algoritmos de ordenamiento básicos y experimenta con su aplicación en registros de seguridad, evaluando tiempos de ejecución y comportamiento frente a diferentes volúmenes de datos. Se analizan resultados para identificar ventajas y limitaciones de cada algoritmo.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	3. Algoritmos de ordenamiento básicos 3.1. Bubble Sort 3.2. Selection Sort 3.3. Insertion Sort 3.4. Estabilidad y costo computacional 3.5. Uso en ordenamiento de registros y logs de seguridad
			4	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante realiza prácticas experimentales de comparación entre algoritmos de búsqueda y ordenamiento, utilizando métricas de eficiencia y escenarios simulados de monitoreo de seguridad. Los resultados obtenidos se integran como cierre del Reto 1.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	4. Análisis algorítmico aplicado a ciberseguridad 4.1. Comparación de algoritmos de búsqueda y ordenamiento 4.2. Medición empírica de eficiencia 4.3. Impacto del algoritmo en sistemas de monitoreo 4.4. Criterios técnicos de selección algorítmica 4.5. Cierre del Reto 1
	RETO 2 – Optimización del procesamiento y organización de la información (Reto formativo) En el segundo reto, el estudiante profundiza en la implementación de algoritmos más eficientes y estructuras de datos jerárquicas, orientadas a mejorar el rendimiento del sistema. Se incorporan algoritmos de ordenamiento avanzados y árboles como mecanismos para optimizar la búsqueda y organización de información. Este reto busca que el estudiante no solo implemente soluciones funcionales, sino que analice su eficiencia computacional y reflexione sobre su aplicabilidad en escenarios donde se manejan grandes volúmenes de datos de seguridad.	Desarrollar algoritmos y estructuras de datos avanzadas para la resolución de problemas de complejidad media-alta, considerando criterios de eficiencia computacional en escenarios de ciberseguridad.	5	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante implementa algoritmos de ordenamiento avanzados y experimenta con su aplicación en grandes volúmenes de datos de seguridad, evaluando mejoras de rendimiento frente a algoritmos básicos mediante pruebas prácticas.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	5. Algoritmos de ordenamiento avanzados 5.1. Merge Sort 5.2. Quick Sort 5.3. Heap Sort 5.4. Comparación con métodos básicos 5.5. Aplicaciones en grandes volúmenes de datos de seguridad
			6	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante desarrolla experimentos de optimización algorítmica, ajustando estrategias de búsqueda y procesamiento para reducir la complejidad temporal en escenarios de alta carga de eventos de seguridad.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	6. Optimización de búsqueda y procesamiento 6.1. Estrategias de optimización algorítmica 6.2. Reducción de complejidad temporal 6.3. Procesamiento eficiente de eventos masivos 6.4. Análisis de rendimiento en escenarios de ataque 6.5. Uso estratégico de estructuras auxiliares
			7	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante implementa árboles binarios de búsqueda y realiza prácticas de inserción, búsqueda y recorrido, experimentando con su uso en la organización jerárquica de información relacionada con la seguridad informática.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	7. Introducción a árboles 7.1. Concepto de árbol y terminologia 7.2. Árboles binarios 7.3. Árboles binarios de búsqueda (BST) 7.4. Inserción, búsqueda y recorrido 7.5. Uso de árboles en organización jerárquica de información
			8	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante experimenta con árboles balanceados desde un enfoque conceptual y práctico, comparando su eficiencia frente a estructuras no balanceadas. Los resultados se consolidan como parte del cierre del Reto 2.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	8. Árboles balanceados y eficiencia 8.1. Problema del desbalance en árboles 8.2. Concepto de balanceo 8.3. Árboles AVL (enfoque conceptual) 8.4. Comparación entre árboles y listas 8.5. Cierre del Reto 2
	RETO 3 – Modelado estructural de escenarios de ciberseguridad (Reto formativo) El tercer reto se centra en el modelado estructural de la información, utilizando árboles y grafos para representar relaciones, dependencias y flujos dentro de un escenario de ciberseguridad. El estudiante emplea estas estructuras para modelar infraestructuras de red, rutas de ataque, relaciones entre eventos o dependencias entre componentes críticos. En este punto, el estudiante comienza a seleccionar y justificar las estructuras de datos más adecuadas según el problema planteado, integrando análisis conceptual y técnico.	Seleccionar las estructuras de datos más adecuadas según los requerimientos y caracteristicas de distintos escenarios de ciberseguridad.	9	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante desarrolla prácticas de modelado de amenazas mediante árboles de decisión y árboles de ataque, experimentando con la representación estructurada de escenarios de ciberseguridad.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	9. Árboles aplicados a la ciberseguridad 9.1. Árboles de decisión 9.2. Árboles de ataque (Attack Trees) 9.3. Modelado de amenazas 9.4. Análisis de rutas de ataque 9.5. Evaluación de nodos críticos
			10	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante implementa grafos para representar infraestructuras y relaciones de red, experimentando con distintas formas de representación y analizando su impacto en el modelado de sistemas de seguridad.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	10. Introducción a grafos 10.1. Definición de grafo 10.2. Grafos dirigidos y no dirigidos 10.3. Grafos ponderados y no ponderados 10.4. Representación mediante listas y matrices 10.5. Grafos en modelado de redes
			11	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante aplica recorridos DFS y BFS sobre grafos, realizando experimentos prácticos para analizar la propagación de eventos o ataques en una red simulada.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	11. Recorridos en grafos 11.1. Búsqueda en profundidad (DFS) 11.2. Búsqueda en anchura (BFS) 11.3. Comparación DFS vs BFS 11.4. Uso de recorridos en análisis de propagación de ataques 11.5. Recursividad implícita en recorridos
			12	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante implementa algoritmos avanzados de grafos, como Dijkstra, y experimenta con el análisis de rutas críticas y caminos mínimos en escenarios de infraestructura comprometida.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	12. Algoritmos avanzados de grafos 12.1. Caminos mínimos 12.2. Algoritmo de Dijkstra 12.3. Análisis de rutas críticas 12.4. Optimización de recorridos 12.5. Aplicaciones en análisis de infraestructuras comprometidas
			13	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante desarrolla prácticas experimentales de análisis forense y detección de nodos críticos utilizando grafos, integrando los resultados como cierre del Reto 3.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cosulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	13. Grafos en escenarios de ciberseguridad 13.1. Modelado de infraestructuras de red 13.2. Detección de nodos críticos 13.3. Dependencias y puntos únicos de falla 13.4. Análisis forense basado en grafos 13.5. Cierre del Reto 3

	RETO 4 – Sistema integrado de análisis de ciberseguridad (Reto sumativo – Proyecto final) El reto final corresponde a la integración completa del sistema, consolidando los aprendizajes desarrollados a lo largo de la asignatura. El estudiante integra algoritmos de búsqueda, algoritmos de ordenamiento, árboles y grafos en una solución funcional orientada a un escenario realista de ciberseguridad. Este reto requiere justificar técnicamente las decisiones de diseño, analizar la eficiencia del sistema y presentar el proyecto como una solución coherente, robusta y alineada con los principios de la ingeniería y la seguridad informática. Este reto constituye la evaluación sumativa de la asignatura y evidencia el logro de los resultados de aprendizaje del nivel.		14	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante realiza experimentos comparativos para seleccionar la estructura de datos más adecuada según distintos escenarios de ciberseguridad, justificando técnicamente sus decisiones de diseño.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cesulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	14. Selección de estructuras de datos 14.1. Criterios de selección de estructuras 14.2. Comparación entre listas, Arboles y grafos 14.3. Trade-offs de diseño 14.4. Justificación técnica de decisiones 14.5. Diseño estructural del sistema final
			15	Tutorias asincrónicas por mensajes, videos, podcast, correos electrónicos, foros, chats.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante integra algoritmos y estructuras de datos en un sistema funcional, realizando pruebas experimentales de rendimiento, escalabilidad y coherencia del diseño como preparación del proyecto final.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cesulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	15. Integración de estructuras de datos 15.1. Integración de búsqueda, ordenamiento, Árboles y grafos 15.2. Arquitectura del sistema de análisis de seguridad 15.3. Evaluación de eficiencia global 15.4. Escalabilidad y mantenibilidad 15.5. Preparación del proyecto final
			16	Tutorias sincrónicas por videoconferencia.	2	Computadora, acceso a internet, acceso al aula virtual, compilador y/o intérprete.	Entorno virtual de aprendizaje, weblabs, software especializado	El estudiante ejecuta pruebas finales del sistema desarrollado, valida su funcionamiento mediante experimentación controlada y presenta los resultados como parte de la defensa del proyecto final.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o software especializado.	Entorno virtual de aprendizaje, weblabs, software especializado	Cesulta e investigación, resolución de problemas de programación sobre el tema en estudio	4,5	Computador con software especializado, compilador y/o intérpete, depurador, aula virtual, Tics, Bibliografia	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	16. Proyecto final y defensa 16.1. Integración completa del sistema 16.2. Validación técnica del diseño 16.3. Análisis algorítmico del sistema 16.4. Presentación y defensa del proyecto 16.5. Reflexión final desde la ciberseguridad

8. BIBLIOGRAFÍA

a. BÁSICA / LIBROS

Bibliografía (basarse en normas APA)	Código Biblioteca PUCESI	Nro. de ejemplares
https://elibro.puce.elogim.com/es/ereader/puce/230298	Biblioteca virtual	NA
https://puce.odilo.us/info/enciclopedia-de-microsoft-visual-c-interfaces-graficas-y-aplicaciones-para-internet-con-windows-forms-y-aspnet-03127168	Biblioteca virtual	NA
https://puce.odilo.us/info/c-5-y-visual-studio-2013-los-fundamentos-del-lenguaje-03126174	Biblioteca virtual	NA
https://puce.odilo.us/info/facil-aprendizaje-estructuras-de-datos-algoritmos-c-aprenda-facilmente-estructuras-de-datos-graficamente-03127232	Biblioteca virtual	NA
https://puce.odilo.us/info/aprende-c-en-un-fin-de-semana-03105596	Biblioteca virtual	NA

Elaborado por:

Damián Nicolalde R

f) Docente

Revisado y Aprobado por:

Damián Nicolalde R
Coordinador de la carrera