PUCE
ESCUELA DE CIENCIAS FÍSICAS Y MATEMÁTICA
CIBERSEGURIDAD • ECUACIONES DIFERENCIALES ORDINARIAS
Emilse Camacho • Semestre 2025-2

PROYECTO FINAL INTEGRADOR

Modelado y análisis de fenómenos dinámicos de ciberseguridad mediante ecuaciones diferenciales

1. Introducción

El presente proyecto final integrador constituye la culminación del proceso de aprendizaje de la asignatura Ecuaciones Diferenciales aplicadas a Ciberseguridad. A lo largo del curso, los estudiantes desarrollaron un proyecto progresivo estructurado en cuatro retos que abordaron distintas fases del modelado matemático y computacional de fenómenos dinámicos propios de la ciberseguridad. Este proyecto tiene como objetivo demostrar la capacidad del estudiante para aplicar ecuaciones diferenciales en el análisis de sistemas complejos, integrando modelado, resolución analítica, simulación y análisis integral.

2. Descripción general del proyecto

El proyecto final tiene como propósito modelar y analizar fenómenos dinámicos de ciberseguridad mediante ecuaciones diferenciales, desarrollándose en cuatro etapas correspondientes a los retos de: (1) modelado de amenazas básicas, (2) análisis de ataques avanzados, (3) simulación de sistemas de seguridad y (4) integración de escenarios complejos. En cada etapa, los estudiantes aplican conceptos teóricos y herramientas computacionales para representar matemáticamente los procesos de ataque y defensa digital, analizar su comportamiento dinámico y presentar conclusiones fundamentadas.

3. Síntesis de las fases previas

• Reto 1 – Modelado de amenazas básicas:

Los estudiantes formularon modelos diferenciales de primer orden que describen la propagación de amenazas informáticas como malware, gusanos o spam, identificando variables, parámetros y condiciones iniciales relevantes.

• Reto 2 – Resolución analítica del modelo formulado en el Reto 1:

Se aplicaron métodos analíticos de resolución (separación de variables, ecuaciones lineales y exactas) para obtener soluciones que permitan interpretar la evolución temporal de las amenazas, evaluando la coherencia entre el modelo y el fenómeno representado.

• Reto 3 – Simulación computacional de sistemas de defensa:

En esta fase se construyeron modelos de segundo orden que representan la respuesta dinámica de sistemas de defensa como firewalls o sistemas IDS/IPS ante ataques. Se realizaron simulaciones computacionales para analizar la estabilidad y la efectividad del sistema frente a diferentes escenarios de amenaza.

4. Fase final – Reto 4: Integración de escenarios complejos

El Reto 4- constituye la última fase del proyecto integrador. En esta etapa, los estudiantes combinarán los aprendizajes previos para construir un modelo integral de ciberseguridad que incluya múltiples vectores de ataque y mecanismos de defensa interconectados. El propósito es analizar el comportamiento global del sistema aplicando transformadas de Laplace y sistemas de ecuaciones diferenciales.

Propósito del reto

Integrar los conocimientos teóricos y prácticos adquiridos en los retos anteriores para modelar y analizar un escenario complejo de ciberseguridad, utilizando transformadas de Laplace y sistemas de ecuaciones diferenciales para representar interacciones dinámicas entre ataques múltiples y sistemas defensivos.

Instrucciones generales

Fase 1 — Compromiso. Cada grupo desarrollará un modelo integral que combine al menos dos tipos de amenazas (por ejemplo, malware y phishing) y dos mecanismos de defensa (por ejemplo, firewall y IDS). Se deberán formular y resolver sistemas de ecuaciones diferenciales que representen las interacciones entre los distintos componentes, y analizar su comportamiento global mediante transformadas de Laplace.

• Seleccionar y describir los ataques y sistemas de defensa a integrar.

• Identificar las variables y parámetros relevantes del modelo.

• Definir los objetivos del análisis integral y su alcance computacional.

Producto parcial: esquema conceptual y justificación del modelo integral.

Fase 2 — Investigación

• Formular el sistema de ecuaciones diferenciales que represente el escenario seleccionado.

• Aplicar transformadas de Laplace para resolver el sistema y analizar su estabilidad.

• Realizar simulaciones computacionales que muestren la evolución temporal de los ataques y defensas.

• Documentar los resultados obtenidos con gráficos y análisis interpretativo.

Producto parcial: simulación y reporte de resultados iniciales.

Fase 3 — Acción

• Analizar el comportamiento dinámico del sistema completo, identificando puntos de equilibrio, oscilaciones y estabilidad.

• Evaluar la efectividad del modelo comparando distintos escenarios de ataque y defensa.

• Preparar el informe técnico y la presentación final del proyecto.

Entregable final: informe técnico completo, archivo de simulación y presentación oral o video de sustentación (5–10 minutos).

5. Evaluación del proyecto final integrador

Dimensión	Evidencia	Indicadores	Peso
Conceptual	Informe técnico global	Integra los conceptos teóricos de los cuatro retos en un modelo coherente y fundamentado.	30 %
Metodológica	Simulación y resolución	Aplica correctamente transformadas de Laplace y métodos numéricos en la simulación del sistema integral.	35 %
Reflexiva	Análisis e interpretación	Analiza críticamente los resultados obtenidos, valorando la estabilidad, la eficiencia y la aplicabilidad del modelo propuesto.	35 %

6. Entregables globales

• Informe técnico final (10–12 páginas) que contenga los modelos formulados, soluciones analíticas, simulaciones y análisis integral.
• Código o archivos de simulación (.py, .ggb o equivalente) debidamente documentados.
• Presentación o video explicativo que sintetice el proceso y los resultados.
• Ficha de autoevaluación grupal y referencias bibliográficas.

7. Competencias transversales

Razonamiento lógico y analítico, pensamiento crítico, modelado matemático aplicado, trabajo colaborativo, comunicación científica y ética profesional en el uso de herramientas tecnológicas para el análisis de sistemas de ciberseguridad.

8. Observaciones metodológicas

• El proyecto integra las cuatro fases desarrolladas durante el curso y constituye la evidencia global de aprendizaje.
• Los grupos deben mantener coherencia entre el modelo formulado en los primeros retos y la integración final.
• Se prioriza la comprensión conceptual, la interpretación de resultados y la claridad de la comunicación científica sobre la complejidad del código empleado.
• Todas las referencias teóricas, modelos y herramientas utilizadas deben citarse de acuerdo con las normas académicas vigentes.