RETO 3 – RDA 3

Simulación computacional de sistemas de defensa en ciberseguridad mediante ecuaciones diferenciales de segundo orden

---

Resultado de aprendizaje (RDA 3)

Aplicar ecuaciones diferenciales de segundo orden para modelar, analizar y simular sistemas dinámicos que representen mecanismos de defensa o respuesta en el contexto de la ciberseguridad.

Criterios de evaluación:

1. Plantea correctamente un modelo de segundo orden que represente un proceso dinámico de defensa o control.
2. Implementa y ejecuta la simulación computacional del modelo en un entorno digital (Python, GeoGebra, MATLAB o equivalente).
3. Analiza e interpreta los resultados obtenidos, valorando la estabilidad y el comportamiento del sistema bajo distintos escenarios.

Propósito del reto

Desarrollar la capacidad de modelar y simular **sistemas de defensa ante ciberataques** utilizando ecuaciones diferenciales de segundo orden.
El reto invita a los estudiantes a comprender cómo los mecanismos de seguridad —como *firewalls, sistemas de detección de intrusos (IDS/IPS)* o *antivirus inteligentes*— reaccionan dinámicamente frente a amenazas externas, y cómo su comportamiento puede evaluarse mediante simulaciones matemáticas.

A diferencia de los retos anteriores, en este desafío se cambia el enfoque desde la **propagación de la amenaza** hacia la **respuesta del sistema**, permitiendo estudiar la estabilidad, la velocidad de reacción y la efectividad de las medidas de defensa.

Instrucciones:

Cada grupo seleccionará un **mecanismo de defensa digital** (por ejemplo, firewall, IDS, IPS, antivirus o honeypot) y planteará un modelo de **ecuación diferencial de segundo orden** que describa su comportamiento dinámico frente a un ataque.
El modelo podrá representarse de manera simbólica y simularse computacionalmente en un entorno digital, analizando cómo los parámetros del sistema afectan su desempeño.

Se sugiere utilizar herramientas de código libre como **Python (Jupyter/Colab)** o **GeoGebra** para la simulación y visualización de los resultados.

Fase 1 — Compromiso

Actividades:

- Revisar los conceptos de ecuaciones diferenciales de segundo orden y sus soluciones características.
- Seleccionar el tipo de defensa digital a modelar (por ejemplo, firewall o IDS).
- Identificar las variables y parámetros que intervienen en el proceso (nivel de detección, tiempo de respuesta, intensidad del ataque, etc.).
- Plantear la ecuación diferencial de segundo orden que represente el comportamiento dinámico del sistema de defensa.

Producto parcial:

Descripción del fenómeno de defensa seleccionado y formulación del modelo diferencial de segundo orden con justificación de variables y parámetros.

Fase 2 — Investigación

Actividades:

- Implementar el modelo en un software de simulación (Python, GeoGebra, MATLAB o equivalente).
- Analizar las soluciones del modelo para diferentes valores de los parámetros.
- Generar gráficos o animaciones que representen la evolución temporal del sistema (por ejemplo, velocidad de reacción, oscilaciones, estabilidad).
- Discutir la correspondencia entre el modelo y el comportamiento esperado del sistema real.

Producto parcial:
Archivo de simulación digital (.py, .ggb o equivalente) acompañado de una interpretación preliminar del comportamiento dinámico.

Fase 3 — Acción

Entregables finales:

- **Informe técnico (3–5 páginas)** que contenga:
  - Descripción del sistema de defensa y su relevancia en ciberseguridad.
  - Modelo matemático formulado y justificación de parámetros.
  - Resultados de la simulación computacional (gráficos, tablas o animaciones).
  - Análisis e interpretación de los resultados, destacando estabilidad, eficiencia y posibles limitaciones del modelo.
- **Presentación o video breve (5–7 minutos)** que muestre la simulación y explique los hallazgos principales.

Evaluación del reto

Dimensión	Evidencia	Indicadores	Peso
Conceptual	Informe técnico	Plantea correctamente la ecuación diferencial de segundo orden y justifica la elección de variables y parámetros.	35 %
Metodológica	Simulación computacional	Implementa adecuadamente el modelo en software, representando el comportamiento del sistema de defensa.	35 %
Reflexiva	Análisis e interpretación	Analiza la estabilidad y la respuesta del sistema, interpretando los resultados en el contexto de la ciberseguridad.	30 %

Competencias transversales

Pensamiento crítico y analítico, modelado matemático aplicado, comunicación técnica escrita y digital, trabajo colaborativo y uso ético de herramientas de simulación.

Observaciones metodológicas

- En este reto se **introduce el uso de ecuaciones de segundo orden** para representar dinámicas más complejas, vinculadas con la **reacción o defensa de un sistema informático**.
- El grupo puede inspirarse en modelos clásicos de oscilación y estabilidad, adaptándolos al contexto digital (por ejemplo, modelos de respuesta amortiguada o resonante).
- La simulación debe priorizar la **interpretación del comportamiento** sobre la complejidad del código: se valora la comprensión conceptual y la coherencia del modelo.
- Los resultados deben presentarse con lenguaje técnico claro y fuentes bibliográficas de respaldo.