

# Algoritmo pseudoaleatorio

Actividad evaluada n°5 IIC1001-1

Martín Pizarro

May 2025

## 1 Introducción

### ¿Qué es?

El **Algoritmo pseudoaleatorio** es un tipo de algoritmo diseñado para generar números de carácter *casi aleatorios* a base de una 'semilla', la cual puede ser reproducida, este algoritmo surgió a base de la necesidad de generar números aleatorios sin los costos de tiempo y poder computacional que conllevan el generar un número verdaderamente aleatorio.

### Origen

El **Algoritmo pseudoaleatorio** fue creado por John von Neumann (1903 - 1957), a través de el " *Método del cuadrado medio*", método el cual utiliza una semilla inicial que es elevada a su cuadrado, para luego utilizar los dígitos centrales de el resultado para una nueva semilla. Este proceso se repite hasta obtener una secuencia de números pseudoaleatorios la cual satisface las necesidades.



## 2 Algoritmo

El algoritmo usado dentro de el repositorio consiste en una versión de el algoritmo pseudoaleatorio creado por Leonardo Schunck Rainha, en su publicación de Generar numeros pseudo-aleatorios en python desde 0. Su método para generar numeros a través de un **Generador lineal de congruencia**, permitiendo el ingreso de una *seed*, o sea, un valor que permite al generador volver a generar un mismo número obtenido previamente. Este algoritmo también permite el entregar un rango como parámetro, el cual le permite al algoritmo limitar el mínimo y máximo valor que puede tener el número aleatorio.

## 3 Referencias

Elena Almaraz Luengo "A brief and understandable guide to pseudo-random number generators and specific models for security," Statistics Surveys, Statist. Surv. 16(none), 137-181, (2022)

Rainha, L. S. (2024, 28 noviembre). Generate pseudo-random number in Pythom from scratch. Medium. <https://medium.com/@schunckrainhaleonardo/generate-pseudo-random-number-in-pythom-from-scratch-e57bb99de981>