Diego Esteban Quintero Rey
Modelos estocásticos y simulación en computación y comunicaciones
ME01
Proyecto Final: Implementación de un enfoque basado en teoría de juegos para contrarrestar amenazas persistentes avanzadas

# MANUAL DE USUARIO Y TÉCNICO

## REQUISITOS

- Contar con una cuenta de Google que le permita interactuar con el notebook de Google Colab
- Descargar el código del proyecto `APT-GT.zip` desde el correo electrónico y hacer la descompresión correspondiente, o clonar el repositorio este6an13/APT-GT (github.com) en su entorno local.
- Subir el notebook `APT-GT.ipynb` a su cuenta de Google Colab
- Subir los archivos auxiliares `exploits_controls.json` y `vulns_exploits.json` al manejador de archivos de Google Colab.

## EJECUCIÓN

- Dirigirse a la pestaña `Runtime` de Google Colab y seleccionar la opción `Run all`. Alternativamente puede ejecutar la combinación de teclas `Ctrl+F9`.

Para ejecutar un experimento dependiente de la topología, el usuario debe definir los siguientes parámetros:

- número de nodos,
- nodo origen,
- nodo objetivo,
- número máximo de ataques a considerar $m$,
- número máximo de controles a considerar $n$.

Si se desea ejecutar un experimento que no depende de la topología, como el del artículo [1]. El usuario solamente necesita definir los siguientes parámetros:

- matriz de distribuciones
- estrategias del atacante
- estrategias del defensor

## MODIFICACIÓN

- El usuario puede extender y modificar la implementación que se encuentra en el notebook a su gusto y de acuerdo con sus necesidades. Se recomienda hacer una copia del notebook para hacer los cambios o tener como referencia el archivo original del proyecto/repositorio para remitirse a él en caso de ser necesario.
- Se invita al usuario a agregar los siguientes parámetros al sistema: número de expertos, número de categorías, máximo orden de las derivadas, umbral de riesgo.
- Se invita al usuario a implementar una función de reporte y una función principal (main).
- Se invita al usuario a definir un parámetro que le permita al usuario decidir qué tipo de experimento utilizar: dependiente de la topología o independiente de la topología.

- El usuario puede también modificar o reemplazar los diccionarios JSON según las necesidades de su análisis.

## REFERENCIAS

[1] Rass S, König S, Schauer S (2017) Defending Against Advanced Persistent Threats Using Game-Theory. PLOS ONE 12(1): e0168675. https://doi.org/10.1371/journal.pone.0168675