Inteligencia Artificial

Trabajo Práctico N° 1: Redes Neuronales

Fecha de entrega: 2/06/2025

Objetivo

Diseñar, entrenar y evaluar modelos de aprendizaje automático que permitan a un agente inteligente aprender a partir de datos estructurados para alcanzar un objetivo determinado. En este caso, el objetivo será clasificar tipos de incidentes de ciberseguridad mediante una red neuronal. Se buscará consolidar el vínculo entre el análisis de datos y las técnicas de aprendizaje automático (machine learning), enfocándose tanto en aspectos teóricos como prácticos del diseño y evaluación de modelos.

Descripción

Durante la cursada de **Ciencia de Datos (CD)** se trabajó sobre un conjunto de datos relacionado con incidentes de ciberseguridad, aplicando técnicas de análisis exploratorio, limpieza, balanceo y transformación de datos. A partir del dataset preprocesado en esa materia (sin valores atípicos, balanceado, con variables seleccionadas y transformadas), se propone continuar el trabajo desde la perspectiva de la **Inteligencia Artificial (IA)**.

El objetivo es construir y evaluar un modelo de red neuronal multicapa (MLP - *Multi-Layer Perceptron*) que permita clasificar adecuadamente los incidentes registrados en el dataset. Para ello, deberán realizarse las siguientes actividades:

Actividades

1. **Diseño del modelo**
   - Diseñar una red neuronal MLP utilizando una librería de aprendizaje profundo (por ejemplo, TensorFlow/Keras o PyTorch).
   - Justificar las decisiones de diseño: número de capas ocultas, cantidad de neuronas por capa, funciones de activación, etc.
   - Utilizar los mismos conjuntos de entrenamiento y validación generados en CD para entrenar y evaluar el modelo.
2. **Ajuste de hiperparámetros**
   - Explorar diferentes combinaciones de hiperparámetros: tasa de aprendizaje, tamaño del batch, número de épocas, función de pérdida, optimizador, regularización (dropout, L2, etc.).

   - Documentar cómo estos cambios afectan la performance del modelo.
3. **Evaluación del modelo**
   - Proponer y calcular métricas apropiadas para evaluar el modelo (por ejemplo: accuracy, precision, recall, F1-score, AUC-ROC).
   - Graficar y analizar las curvas de aprendizaje (loss y accuracy) para entrenamiento y validación.
4. **Comparación con modelos tradicionales**
   - Comparar la performance del modelo MLP con los modelos tradicionales utilizados en CD.
   - Analizar las diferencias en términos de:
     - Métricas de clasificación
     - Tiempo de entrenamiento
     - Requerimientos computacionales (memoria, GPU/CPU)
5. **Conclusiones**
   - Reflexionar sobre los desafíos y ventajas del uso de redes neuronales en comparación con métodos más clásicos.
   - Proponer mejoras o líneas futuras de trabajo para modelos más complejos (por ejemplo: redes convolucionales, modelos recurrentes, transfer learning, etc.), si correspondiera al tipo de datos.

Documentación a presentar:

Se deberá elaborar un informe técnico con el formato propuesto en el ***Anexo I***.

ANEXO I: Formato del informe del TP

Nombre del TP

Nro. de Grupo

Nombre y Apellido integrante1 - e-mail
Nombre y Apellido integrante2 - e-mail
Nombre y Apellido integrante3 - e-mail

Resumen. Acá se escribe un pequeño resumen del trabajo que se presenta. Por ejemplo, la aplicación de IA que se va a hacer, el problema concreto que se va a resolver, si fue o no resuelto y cómo, y los resultados que se presentan. Todo en pocas palabras (entre 70 y 150 palabras).

1 Introducción

En esta sección se introduce el área de aplicación en la que se va a trabajar, se explica el problema que se va a resolver. Se puede usar una figura o esquema para explicar mejor lo que se quiere hacer en el trabajo.
Se puede mostrar un gráfico con los datos que se están usado. En ese caso se diría p.e. "los datos usados para el entrenamiento se pueden ver en la figura 1, ... Esto quiere decir que …". Esta forma de nombrar los gráficos se mantiene para todo el informe, es decir, se usará este formato cada vez que se presente una figura.

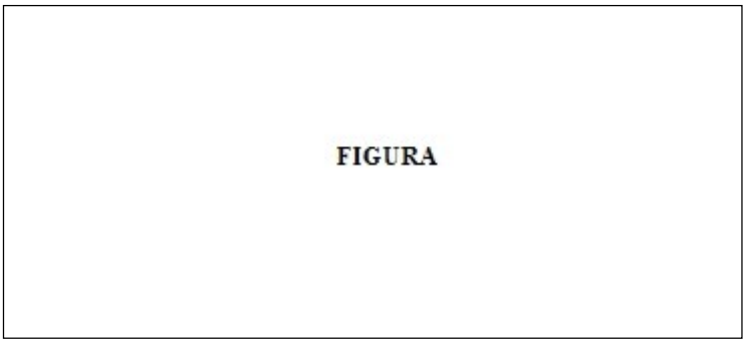

Figura 1. Explicación de lo que se ve en la figura.

Si los datos o alguna otra información a lo largo del trabajo se quiere presentar en forma de tabla, acá se muestra un formato posible como ejemplo.

XX	XXXX	
Col 1	Col 2	Col 3
xxx	xx.xx	xx.xx
xxx	xx.xx	xx.xx
xxx	xx.xx	xx.xx
xxx	xx.xx	xx.xx

Tabla 1. Explicación de lo que se ve en la tabla.

Generalmente, al final de la introducción se describe cómo sigue el informe, es decir, se explica que hay en cada sección siguiente. Por ejemplo: " en la sección 2 se explica ... . En la sección 3 se muestra ... . Finalmente en la sección xx …".

2 Solución

En esta parte se debería explicar la solución conceptual del problema (estado del agente, estado inicial y final del agente, estado del ambiente, percepciones, prueba de meta, operadores, heurística, estrategia seleccionada). Si se aplicó alguna metodología para resolver el problema, explicarla.
Justificar la solución y las elecciones hechas.
Si se va a hacer alguna comparación, explicar entre qué cosa y qué cosa, y por qué se comparan.
Mostrar por ejemplo algún gráfico con el modelo del problema resuelto.
Si se quiere escribir alguna ecuación, la forma de hacerlo se muestra acá abajo. Se coloca la ecuación en el texto (*es un objeto equation en word*) y a la derecha se pone un número para identificarla, que aumenta secuencialmente a medida que se agregan más ecuaciones al informe.

$$y = x \tag{1}$$

3 Resultados

En esta sección se deberían mostrar las pruebas que se han hecho para verificar que la solución al problema propuesto funciona y explicar los resultados obtenidos.
Se deben mostrar los resultados obtenidos para una ejecución con el ciclo percepción, actualización del estado, acción.
Se pueden mostrar gráficos o tablas con los resultados obtenidos de las ejecuciones, con los errores obtenidos, etc.
Si se trató de resolver un problema, hay que mostrar cómo el agente lo resolvió (o no), o si se buscaba una respuesta a una pregunta, cuál es la respuesta que brinda el agente propuesto.

4 Conclusiones

En esta sección se deben obtener conclusiones del trabajo presentado.
Que conclusión se puede sacar luego de haber aplicado una técnica de IA para resolver un problema.
Si el modelo propuesto para resolver el problema es bueno o no, por qué, ventajas, desventajas, puntos positivos, puntos negativos, etc…

ACLARACION: este documento pretende ser de base en cuanto al FORMATO del trabajo práctico, es decir, el tipo de letra, tamaño, como mostrar figuras y tablas, etc., para uniformar las presentaciones de los distintos grupos. Los nombres de las secciones son sugerencias, no etiquetas obligatorias. Cada grupo elegirá la cantidad y nombres de secciones y el tipo y cantidad de información que agregará al informe, según el problema que haya (o no) resuelto.

Referencias (aclaración: si se consultaron libros, o papers, o se bajaron datos de internet, etc., se deben colocar las referencias en esta sección)

1. Apellido, Nombre: Nombre LIBRO. Editorial (año)
2. Apellido, Nombre: Nombre PAPER. Nombre REVISTA o CONGRESO, volumen, numero, nro. de paginas (desde-hasta), (año)

EJEMPLOS

1. Martin del Brio, B., Sanz Molina, A.: Redes Neuronales y sistemas difusos. Ed. Alfaomega (2002)

2. Meireles, M.R.G., Almeida, P.E.M., Simoes, M.G.: A comprehensive review for the industrial applicability of Artificial Neural Networks. IEEE Transactions on Industrial Electronics, vol. 5, no. 3, pp. 585-601 (2003)
3. http://www.iee.org