# Funcionamiento del Aprendizaje Automático

## 1. ¿Qué es el Aprendizaje Automático?

El aprendizaje automático (machine learning) es un subcampo de la inteligencia artificial que se centra en la creación de algoritmos que permiten a las computadoras aprender patrones a partir de datos. En lugar de ser programadas explícitamente para realizar tareas, las máquinas utilizan datos para "aprender" y hacer predicciones o tomar decisiones.

## 2. Estructura del Proceso de Aprendizaje

El proceso de aprendizaje automático generalmente sigue estos pasos:  
  
a. Recolección de Datos  
Se recolectan datos que se utilizarán para entrenar el modelo. En este caso, serían correos electrónicos con etiquetas que indican si son maliciosos o seguros. Estos datos se almacenan en un formato estructurado, como un archivo CSV o una base de datos.  
  
b. Preparación de Datos  
Los datos crudos se procesan para convertirlos en un formato que pueda ser utilizado por el modelo. Esto incluye limpieza (como eliminar caracteres especiales), normalización (como convertir todo a minúsculas) y selección de características (como usar TF-IDF para vectorizar texto).  
  
c. División de Datos  
Los datos se dividen en conjuntos de entrenamiento y prueba. El conjunto de entrenamiento se utiliza para entrenar el modelo, mientras que el conjunto de prueba se utiliza para evaluar su rendimiento.  
  
d. Entrenamiento del Modelo  
Se elige un algoritmo de aprendizaje automático (como Naive Bayes en este caso) y se alimenta con el conjunto de entrenamiento. El modelo "aprende" ajustando sus parámetros internos para minimizar el error en las predicciones. Esto se hace mediante un proceso llamado optimización, que ajusta los pesos de las características basadas en cómo se desempeñan las predicciones en comparación con las etiquetas reales.  
  
e. Evaluación del Modelo  
Una vez que el modelo ha sido entrenado, se evalúa su rendimiento utilizando el conjunto de prueba. Se calculan métricas como precisión, recall y F1-score para entender qué tan bien está funcionando.

## 3. ¿Dónde se Almacena lo que Aprende el Modelo?

Una vez que el modelo ha sido entrenado, sus parámetros y estructura se pueden guardar en un archivo. Esto se hace típicamente utilizando bibliotecas como `joblib` o `pickle` en Python. Aquí hay un ejemplo básico de cómo guardar y cargar un modelo:  
  
```python  
import joblib  
  
# Guardar el modelo  
joblib.dump(model, 'modelo\_emails.pkl')  
  
# Cargar el modelo  
model = joblib.load('modelo\_emails.pkl')  
```  
  
Esto crea un archivo llamado `modelo\_emails.pkl` que contiene todo lo que el modelo ha aprendido.

## 4. Uso del Modelo Entrenado

Una vez que tienes un modelo guardado, puedes usarlo para hacer predicciones sobre nuevos datos. Simplemente cargas el modelo y le pasas los datos que deseas clasificar.  
  
```python  
# Vectorización del nuevo texto  
nuevo\_texto = ["¡Felicidades! Has ganado un premio."]  
nuevo\_texto\_tfidf = vectorizer.transform(nuevo\_texto)  
  
# Predicción  
prediccion = model.predict(nuevo\_texto\_tfidf)  
print(prediccion)  
```  
  
## 5. Actualización del Modelo  
Con el tiempo, es posible que necesites actualizar el modelo con nuevos datos. Esto puede implicar volver a entrenarlo desde cero o ajustarlo con los nuevos datos. El proceso es similar al inicial: recolectar datos, preparar datos, entrenar y evaluar nuevamente.

## 6. Manejo de Datos

Los datos de entrada y las predicciones generadas por el modelo se pueden almacenar en bases de datos o archivos para su análisis posterior. Esto es especialmente útil si deseas realizar análisis a largo plazo o hacer auditorías.

## Resumen

En resumen, el aprendizaje automático implica un ciclo de recolección de datos, preparación, entrenamiento y evaluación. Los parámetros aprendidos se guardan en archivos y se pueden utilizar para hacer predicciones en nuevos datos. Con el tiempo, puedes actualizar el modelo según sea necesario.