Marco Jurado 20308
Christopher Garcia 20541

Discusión Laboratorio 2 Detección de SPAM

1. ¿Qué error es más “aceptable”: dejar pasar un SMS de SPAM (falso negativo) o bloquear un SMS legítimo (falso positivo)? Justifique su respuesta.
    a. Consideramos que es mejor dejar pasar un SMS de SPAM (falso negativo) que bloquear un SMS legítimo (falso positivo). Esto se debe a que bloquear un mensaje legítimo puede impedir que tengamos comunicación que puede ser importante, mientras que recibir un SMS de SPAM, aunque molesto y potencialmente peligroso, suele ser menos crítico.

2. Compare los valores para cada modelo de representación numérico. En base a la respuesta de la primera pregunta ¿Qué modelo de representación numérica produjo el mejor resultado, BoG o TF-IDF? ¿Cuál o cuáles son las razones por las que dicho modelo se comportó de mejor manera?

```
Modelo BOW con n=1
Precisión: 0.9802690582959641
Matriz de Confusión:
 [[960   5]
 [ 17 133]]
Reporte de Clasificación:
              precision    recall  f1-score   support

         ham       0.98      0.99      0.99       965
        spam       0.96      0.89      0.92       150

    accuracy                           0.98      1115
   macro avg       0.97      0.94      0.96      1115
weighted avg       0.98      0.98      0.98      1115
```

```
Modelo BOW con n=2
Precisión: 0.9766816143497757
Matriz de Confusión:
 [[962   3]
 [ 23 127]]
Reporte de Clasificación:
              precision    recall  f1-score   support

         ham       0.98      1.00      0.99       965
        spam       0.98      0.85      0.91       150

    accuracy                           0.98      1115
   macro avg       0.98      0.92      0.95      1115
weighted avg       0.98      0.98      0.98      1115
```

```
Modelo TF-IDF
Precisión: 0.96804149548436 77
Recuerdo: 0.9668161434977578
Puntuación F1: 0.9647940181783204
Reporte de Clasificación:
              precision    recall  f1-score   support

         ham       0.96      1.00      0.98       965
        spam       1.00      0.75      0.86       150

    accuracy                           0.97      1115
   macro avg       0.98      0.88      0.92      1115
weighted avg       0.97      0.97      0.96      1115
```

a. El modelo BoW con n=1 tuvo el mejor equilibrio entre precisión y recall, con una tasa de detección de spam aceptable y la menor cantidad de mensajes legítimos incorrectamente marcados como spam. El modelo BoW con n=2 mostró una reducción en el rendimiento, por la sobresaturación de características y sobreajuste. El modelo TF-IDF tuvo un recall significativamente más bajo para la categoría de spam, lo que significa que dejó pasar más correos electrónicos de spam que

los modelos BoW. Por lo tanto BoW con n=1 parece haber producido el mejor resultado general.

3. En base a la exploración de datos e ingeniería de características que realizó en el primer y este laboratorio, ¿qué consejos le daría a un familiar que le solicita ayuda para detectar si un email o SMS es phishing o no? ¿En qué características de una URL/email podría fijarse su familiar para ayudarlo a detectar un potencial phishing?
    a. Verifica la autenticidad de las urls. Normalmente tiene faltas de ortografía o pueden hacer intercambio de palabras por números como por ejemplo escribir “Hol4”.
    b. Desconfía de los mensajes que solicitan información o privada, sería mejor consultar con la empresa o negocio que se está tratando para asegurar el porqué necesitan esa información.
    c. Los phishers a menudo crean un sentido de urgencia para que les respondas rápido y puedan robarte tu información.
    d. Verifica si conoces al remitente y si el correo electrónico parece legítimo
    e. Ver que la url no contiene muchos símbolos raros que no verías normalmente en una url de página web.
    f. Verificar que la url no sea demasiado larga pues normalmente suelen ser muy largas para evitar que la leas toda y puedas detectar anomalías en la misma.

4. Si detectamos una URL o email/SMS de phishing, ¿qué podemos hacer para detener su distribución?
    a. No hacer clic en enlaces, no descargar archivos adjuntos, ni brindar ninguna información personal.
    b. Muchos servicios de correo electrónico y plataformas tienen opciones para reportar phishing o SPAM.
    c. Informa a tus contactos y a tu red sobre los intentos de phishing para prevenir que sean víctimas. Sin embargo no lo hagas en naturaleza de generar pánico pues esto puede ser penalizado por la ley.