https://doi.org/10.37815/rte.v35n2.1050
Artículos originales

Síntesis Textual de Evaluación para Acoso y Ciberacoso

Textual Synthesis of Test for Bullying and Cyberbullying

Marcos Orellana[1] https://orcid.org/0000-0002-3671-9362, Jorge Luis Zambrano-Martinez[1] https://orcid.org/0000-0002-5339-7860, Patricio Santiago Garcia Montero[1] https://orcid.org/0009-0007-4113-8400, Liliana Marilu Lojano[1] https://orcid.org/0009-0006-4993-8747, Mateo Sebastian Zea[1] https://orcid.org/0009-0005-4209-8143, Tupak Pacjakutik Japon[1] https://orcid.org/0009-0005-3239-992X

[1]*Laboratorio de Investigación y Desarrollo en Informática (LIDI)*
Universidad del Azuay, Cuenca, Ecuador
marore@uazuay.edu.ec, jorge.zambrano@uazuay.edu.ec,
santyg20@es.uazuay.edu.ec, liliana1998@es.uazuay.edu.ec,
mzea582@es.uazuay.edu.ec, tupak.japon@es.uazuay.edu.ec

Enviado: 2023/07/14
Aceptado: 2023/08/15
Publicado: 2023/10/15

Resumen

En los últimos años, el acoso y el ciberacoso son problemas que han aumentado vertiginosamente afectando escuelas, colegios y universidades. Debido a los avances en las tecnologías de la información, cualquier persona está expuesta a ser atacada; por esta razón, es necesario crear soluciones a través de técnicas adecuadas que ayuden a prevenir el acoso y ciberacoso. En consecuencia, en este artículo se propone crear una síntesis textual a partir de datos de encuestas que permita desarrollar modelos para clasificar o predecir tanto a víctimas como agresores de acoso y ciberacoso. Para ello, se utilizaron técnicas de minería de datos, árboles de decisión y técnicas de agrupación, dando como resultado una síntesis textual. Esto permitió la creación y evaluación de un modelo de aprendizaje supervisado y otro modelo con técnicas de agrupamiento, aplicadas a los datos de las encuestas realizadas a estudiantes universitarios. Los resultados demostraron la importancia de la síntesis textual para la generación de modelos de clasificación o predicción de víctimas y agresores del acoso y ciberacoso, con una exactitud mayor al 75%, siendo el modelo de agrupamiento con mejor rendimiento.

Palabras clave: Acoso, Ciberacoso, Minería de datos, Árbol de decisión, Agrupamiento.

Como citar: Orellana, M., Zambrano-Martinez, J. L., Garcia, P. S., Lojano, L. M., Zea, M. S. & Japon, T. P. (2023). Síntesis Textual de Evaluación para Acoso y Ciberacoso. *Revista Tecnológica - Espol, 35(2), 192-205.* Recuperado a partir de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/1050

Abstract

In recent years, bullying and cyberbullying have increased, affecting schools, colleges, and universities. Due to advances in information technology, any person is exposed to being attacked. Therefore, it is necessary to create solutions through appropriate techniques that help prevent bullying and cyberbullying. Consequently, this article proposes to create a textual synthesis from survey data that allows the development of models to classify or predict both victims and aggressors of bullying and cyberbullying. Data mining techniques, decision trees, and grouping techniques were used, resulting in a textual synthesis. This allowed the creation and evaluation of a supervised learning model and another model with clustering techniques applied to the data from the surveys performed on university students. The results demonstrated the importance of textual synthesis for generating models for the classification or prediction of victims and aggressors of bullying and cyberbullying, with an accuracy greater than 75% for the grouping model with the best performance.

Keywords: Bullying, Cyberbullying, Data mining, Decision tree, Clustering.

Introducción

La violencia es un fenómeno global que afecta a la sociedad en varios escenarios de la vida cotidiana, como los hogares, colegios, lugares de trabajo y relaciones personales. Su presencia trae consecuencias negativas en cualquier ámbito, ya sea social, económico, político o gubernamental. No tiene distinción por edad, género, raza, o cultura y puede expresarse de varias formas. Además, tiene un impacto devastador en la vida de la persona que la sufre, alterando aspectos de su salud física y mental. La violencia puede ser verbal, física, sexual, psicológica o de género (Nielsen y Einarsen, 2018). No obstante, una forma que se encuentra a menudo en la sociedad moderna es el acoso, un tipo de violencia que puede ir desde el acoso verbal hasta la agresión física o psicológica e incluso digital, como el ciberacoso (Mollo et al., 2018).

El auge de las redes sociales, juegos en línea y aplicaciones de mensajería instantánea ha evolucionado la forma en que las personas interactúan, sin embargo, han dado lugar a una creciente forma de violencia. El ciberacoso utiliza cualquier medio de difusión digital para acosar, intimidar, chantajear o difamar a una persona, a diferencia del acoso tradicional, que utiliza medios físicos o verbales para el mismo fin. Ambos tipos de violencia están presentes en los mismos escenarios, pero el ciberacoso posee un mayor alcance debido a las crecientes redes digitales y de telecomunicaciones que conectan en la actualidad a la mayoría de la población (Castilla, 2021). Sin embargo, toda esa interacción digital deja grandes cantidades de información que puede ser explorada y explotada mediante técnicas y algoritmos de minería de datos para combatir y mitigar estas formas de violencia.

La minería de datos permite analizar información con el fin de procesar y explorar cualquier patrón o relación no evidente a simple vista (Han et al., 2022). En este estudio se determinó el uso de la minería de datos como una herramienta para analizar y sintetizar los datos de una encuesta aplicada a estudiantes universitarios sobre sus experiencias con el acoso y ciberacoso, aplicando técnicas como el preprocesamiento de datos, técnicas de agrupamiento y modelos de clasificación. La finalidad del estudio es generar una síntesis textual de las ideas primordiales obtenidas de las encuestas que actúe como punto de partida para la generación de conocimiento sobre el acoso y el ciberacoso.

El resto del documento se estructura de la siguiente manera: Sección 2, presenta los trabajos relacionados, la Sección 3 plantea los fundamentos teóricos de la investigación, la

Sección 4 expone los materiales y métodos utilizados, la Sección 5 explica los resultados que se han obtenido luego de aplicar los métodos y la Sección 6 presenta las conclusiones y trabajos futuros.

Trabajos relacionados

La presencia del acoso y el ciberacoso genera gran discusión en la comunidad académica, lo que ha llevado a varios investigadores a trabajar para beneficio de las personas que padecen a diario estas agresiones (Arce-Ruelas et al., 2022). Los trabajos que se exponen a continuación demuestran el uso de la minería de datos y textos en la generación de modelos de detección y clasificación de estos fenómenos.

En el trabajo de Shaikh et al. (2020), desarrollan una revisión sistemática de literatura para identificar los factores que impulsan a estudiantes universitarios hacia el ciberacoso. Su trabajo pretende servir de guía para futuras investigaciones en el análisis del ciberacoso. Identificaron cerca de 35 factores en 32 estudios, siendo los más reportados problemas emocionales (depresión, ansiedad y estrés), autoestima, agresión, personalidad, malas relaciones, estilo de crianza, rendimiento académico, falta de empatía, exposición tecnológica y facilidad de acceso a internet.

Del mismo modo, Namane y Kyobe (2017), a través de la Universidad de Cape Town, relataron el desarrollo de un análisis con respecto al comportamiento y características de las personas agresoras. En el análisis participaron 3,621 personas (víctimas y agresores) con un promedio de edad entre 14 y 18 años. A través de una encuesta, los investigadores demostraron que 407 participantes fueron víctimas de acoso y se separaron en tres índices de riesgo social. Estos índices se comprenden por la probabilidad que una persona sufra de algún perjuicio dentro del entorno que le rodea (Jorgensen y Siegel, 2019). Así, según Namane y Kyobe (2017), 107 participantes fueron víctimas de acoso provenientes de sectores con bajo riesgo social, 114 participantes se ubicaron dentro del medio riesgo social y 186 participantes dentro del alto riesgo social sufrieron acoso. Además, enfatizaron que los comportamientos violentos se presentan con mayor frecuencia en adolescentes, debido a que es una etapa con mucha variación y cambios constantes en la personalidad, actitudes y emociones.

Por lo tanto, los adolescentes se sitúan como uno de los mayores grupos de consumidores y creadores de contenido en las redes sociales, así en el trabajo de (Bozyiğit et al., 2019) se evaluaron ocho modelos distintos de redes neuronales para la detección de ciberacoso en tweets de Turquía. Los investigadores emplearon técnicas de minería de textos para procesar la información como la tokenización, transformación y la eliminación de símbolos, en conjunto con otras técnicas como frecuencia de término – frecuencia inversa de documento (TF-IDF) y N-gramas para procesar 3,000 tweets y entrenar los distintos modelos. Finalmente, solo un modelo presentó una exactitud del 91%, debido a la utilización de varias configuraciones. Los investigadores también demostraron que incrementar el número de capas ocultas no necesariamente mejora el rendimiento del modelo.

Adicionalmente, para implementar un tipo de red neuronal denominada memoria a corto-largo plazo (LSTM) en el trabajo de Mahat (2021), los investigadores utilizaron datos de Twitter, Wikipedia y Formspring. Un total de 9,000 registros fueron procesados con técnicas de minería de textos (eliminación de caracteres especiales, espacios y ruido en general). Al final el modelo tuvo una exactitud del 77.9%. Otra aplicación de modelos de aprendizaje profundo en redes sociales se aprecia en el trabajo de Banerjee et al. (2019), donde utiliza un modelo basado

en una red neuronal convolucional para la detección del ciberacoso en India. Cerca de 69,874 tweets fueron extraídos y procesados para eliminar palabras vacías y signos de puntuación. Posteriormente, los textos fueron vectorizados para alimentar al modelo, que logró una exactitud de 93.97%, superando a otros modelos de aprendizaje automático, como la máquina de vector de soporte (SVM).

En contraste con lo anterior, Dalvi et al. (2020) presenta un método para la detección de ciberacoso que utiliza una SVM y un clasificador Naive Bayes. Recuperaron tweets de locaciones en tiempo real y utilizaron técnicas de preprocesamiento de datos (tokenización, eliminación de signos de puntuación y palabras vacías, lematización y transformación) a través de un paquete de herramientas de lenguaje natural (NLTK). Al final, el algoritmo SVM es el que presenta una mayor exactitud, con el 71.25%, a diferencia del clasificador bayesiano, con 52.70%.

Si bien las redes sociales son utilizadas a menudo en el análisis del acoso y ciberacoso, también existen estudios enfocados a detectarlos en otras plataformas, como los juegos en línea. Cornel et al. (2019) desarrollan una red neuronal convolucional para detectar la presencia de ciberacoso en los registros de mensajería de dos juegos en línea: *Dota y Ragnarok*. A través de varias interfaces de programación de aplicaciones (APIs) recogieron 230,394 frases de Dota pertenecientes a usuarios de Filipinas y 534,328 de usuarios que jugaron *Ragnarok* en Japón y Singapur. Luego de eliminar las palabras vacías y caracteres especiales, vectorizaron los registros a través del algoritmo *word embedding* para alimentar al modelo. La red neuronal tuvo una exactitud de 99.93%, sin embargo, los investigadores concluyeron que el modelo tiende a sobre ajustarse, por lo que recomendaron explorar otros modelos de aprendizaje profundo.

Como se evidencia en los trabajos mencionados, las redes neuronales son utilizadas a menudo en el análisis de estos fenómenos utilizando distintos modelos. De igual forma, Rahman et al. (2021) evalúan los siguientes modelos de aprendizaje automático: SVM, árboles de decisión, bosque aleatorio, regresión logística y clasificador bayesiano. A través de varias plataformas (Kaggle, Twitter, Wikipedia y YouTube) recuperaron 31,403 registros etiquetados como inofensivos, y 23,663 etiquetados como ciberacoso. Para este análisis, se utilizan técnicas de preprocesamiento de datos (limpieza, derivación, eliminación de ruido y palabras vacías) y el valor TF-IDF para construir los modelos. Como resultado, el bosque aleatorio presentó la mayor precisión de todos, con el 89%.

En base a los estudios mencionados, los avances en la detección y clasificación del acoso y ciberacoso van desde el análisis de comportamientos hasta la aplicación de modelos de aprendizaje profundo. Todos ellos emplearon técnicas de minería de datos o textos y algunos de ellos coincidieron en varias tareas de preprocesamiento. Sin embargo, la tarea de síntesis previa de los datos es fundamental, debido a que los datos suelen contener ruido y afectan al rendimiento de los modelos (Tapia et al., 2018). Por lo tanto, son escasos los trabajos que resaltan la importancia y el uso de diferentes técnicas en la síntesis de texto en el análisis del acoso y el ciberacoso.

Marco Teórico

El acoso y el ciberacoso son temas extensos por tratar y abarcan varios campos de la psicología, desde conductas humanas hasta rasgos de personalidad que surgen en edades tempranas, como la niñez y adolescencia. Cuando se presenta, suele repetirse a menudo en ambientes donde el agresor siente confianza y que el agredido suele frecuentar como las

escuelas, colegios, universidades y demás instituciones educativas. Las agresiones van desde insultos, golpes, discriminaciones, burlas, hasta publicaciones de información, fotografías y videos íntimos que buscan difamar y avergonzar a la persona agredida. El ciberacoso utiliza la tecnología como su herramienta principal para agredir de manera pública o anónimamente a su víctima desde cualquier parte del mundo. Estas agresiones pueden incurrir en varios problemas físicos y mentales de la persona agredida, desde falta de confianza, problemas para socializar, depresión hasta lesiones físicas o suicidios (Li et al., 2022).

Tapia et al. (2018) describen al acoso como una conducta intencional carente de ética, inmoral e impropia, que se basa en una serie de amenazas físicas o verbales hacia otra persona, generando angustia en la víctima y un desequilibrio de poder entre su persona y el agresor. Mientras tanto, el ciberacoso es una amenaza que afecta a la sociedad moderna gracias al surgimiento de nuevas tecnologías de información. Si bien el avance tecnológico ha sido de beneficio en áreas críticas como la salud y la educación, también ha generado un problema social grave. El anonimato en la era digital en conjunto con problemas o trastornos de una persona puede resultar en posibles agresores, que perciben la violencia como una salida a su conflictiva realidad. En contraste, la persona agredida tiende a dificultar la comunicación con su entorno, lo que reduce la posibilidad de que algún familiar o una persona de su círculo cercano logre identificar la presencia de ciberacoso fácilmente.

De acuerdo con Herrera et al. (2018), la mayoría de ciber atacantes cursan el segundo y tercer año de secundaria, a diferencia de la mayoría de sus víctimas, que cursan el primer y segundo año. Adicionalmente, la diferencia de edad, el contenido y el tiempo de navegación en internet también resultaron ser factores a tener en cuenta a la hora de identificar a una persona agresora o víctima. Según Martin-Criado et al. (2021), las plataformas y actividades de mayor visita para los menores de edad se centran en las redes sociales y plataformas de video. Su alto consumo hace que los menores tiendan a recrear las situaciones, comportamientos y léxico que se exhiben en dichas plataformas, lo que incrementa la probabilidad de que un menor pueda recrear comportamientos violentos en su entorno.

Por otro lado, la minería de datos es una técnica que se ha popularizado en los últimos años; permite analizar grandes conjuntos de datos con el fin de encontrar y esclarecer cualquier patrón o relación no evidente a simple vista. Entre sus tareas más conocidas se encuentran el análisis, síntesis y visualización de datos. Su finalidad es generar conocimiento sobre temas de interés, ayudar en la toma de decisiones empresariales u optimizar procesos industriales. Con la generación masiva de información actual, las fuentes de datos se pueden encontrar en línea, a través de gestores de bases de datos o se generan mediante encuestas, grupos focales y otras técnicas de recolección. Entre los sectores más interesados en la minería de datos se encuentra el sector empresarial, que aprovecha este proceso para detectar anomalías, fraudes o mejorar sus estrategias comerciales. Existen metodologías maduras que facilitan y estandarizan sus fases, como el descubrimiento de conocimientos en las bases de datos (KDD) con sus seis etapas: selección de datos, preprocesamiento, transformación, minería de datos, evaluación y finalmente interpretación (Schröer et al., 2021).

El preprocesamiento de datos es una tarea que consiste en la limpieza y eliminación del ruido de los datos para ajustarse a técnicas y modelos de minería de datos. Estas tareas mejoran la calidad, consistencia y confiabilidad de los datos al corregir, reemplazar y eliminar datos incorrectos, irrelevantes o redundantes. La transformación, por otra parte, incluye la selección de atributos relevantes en el estudio, así como técnicas de transformación como la discretización, normalización y aumento o reducción de dimensionalidad. Adicionalmente, en caso de tratarse

de un tipo de aprendizaje supervisado, se debe establecer el atributo de salida o etiqueta (Castro R et al., 2018).

El aprendizaje supervisado se utiliza en situaciones específicas en donde se quiere inferir conocimiento a partir de datos etiquetados, es decir, que se conoce su variable a predecir o clasificar. En esta técnica se utilizan los datos etiquetados para entrenar el modelo, y se evalúa con datos no etiquetados para medir su rendimiento. Uno de los modelos utilizados en este estudio y más populares de aprendizaje supervisado es el árbol de decisión, un modelo fácil de implementar e interpretar cuando se configura adecuadamente. Su funcionamiento se basa en la estructura de un árbol, y representa a las características o atributos seleccionados mediante nodos, y a su vez, ramifica las opciones de cada una (Ramirez y Ccallohuari, 2020).

Por otra parte, el aprendizaje no supervisado no dispone de una variable de salida preestablecida, sino que trata de encontrar patrones o relaciones en el conjunto de datos que permitan clasificar, categorizar o etiquetar los registros. Una de las técnicas más utilizadas en el aprendizaje no supervisado y por ende en este estudio es el agrupamiento. Esta técnica trata de generar grupos con registros similares y separar los grupos con características ajenas. Su funcionamiento se basa en el uso de métricas de distancia o similitud, como la euclidiana, coseno, manhattan, entre otras (Roux, 2018). Existen variaciones de esta técnica con diferentes algoritmos internos y la elección de alguna dependerá del tipo de datos y el problema que se quiera afrontar (Bracco, 2018).

Materiales y Métodos

Los materiales necesarios para la aplicación de técnicas y algoritmos de minería de datos en este estudio se describen a continuación:

- Plataforma de minería de datos RapidMiner.
- Conjunto de datos de encuestas sobre experiencias con el acoso y ciberacoso en estudiantes universitarios.

RapidMiner es un software libre y gratuito (en su versión básica) de análisis y minería de datos que cuenta con una interfaz gráfica amigable hacia el usuario y un flujo de trabajo basado en operadores y conexiones, logrando mayor productividad en menos tiempo. Además, cuenta con más de 1,500 operadores que van desde tareas de preprocesamiento hasta técnicas avanzadas de modelado y visualización de datos (Kathuria et al., 2021). Asimismo, es compatible con los formatos de archivos que albergan los conjuntos de datos más utilizados como archivos de Excel. Este tipo de archivo contiene registros de datos de una encuesta realizada a estudiantes universitarios con el fin de recolectar información demográfica, estudiantil y experiencias con el acoso y el ciberacoso. El conjunto de datos cuenta con 702 registros y un total de 55 atributos o columnas.

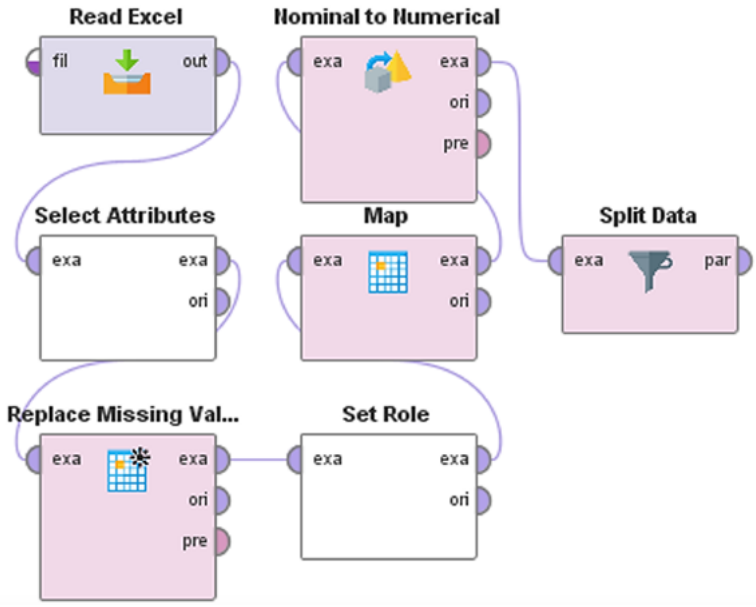
Para aplicar con éxito los procesos y algoritmos de minería de datos en cualquier entorno, es necesario aplicar la metodología KDD (Gupta y Chandra, 2020). Por lo tanto, es imprescindible una fase previa de conocimiento, familiarización y preprocesamiento de los datos, para comprender los tipos de datos, su extensión, longitud, atributos, inconsistencias y el atributo o etiqueta de salida en caso de tratarse de un aprendizaje supervisado (Ruiz-Chávez et al., 2018). La etiqueta es un valor que clasifica o categoriza al registro; en este contexto, un atributo que indica si el encuestado ha sufrido de acoso o ciberacoso. En esta fase se aplicaron los siguientes procesos:

- *Selección de atributos o variables*: se seleccionaron los atributos más relevantes de la encuesta realizada para el análisis y la sintetización textual del acoso y el ciberacoso. Para ello, se analizaron 18 atributos del cuerpo de la encuesta que proporcionan información necesaria para los procesos de agrupamiento y clasificación.
- *Limpieza o preprocesamiento de los datos*: para asegurar la calidad del proceso de minería de datos, los registros con valores nulos fueron identificados e imputados. Este proceso implica reemplazar los valores faltantes por otro valor, variable o estadístico.
- *Transformación de los datos*: muchos algoritmos y modelos de minería de datos requieren ciertos tipos de valores para funcionar correctamente o dar mejores resultados. Algunas de las técnicas de transformación de datos incluyen la discretización, codificación de valores y asignación de nuevos valores. Otra parte fundamental en este proceso es la división del conjunto de datos para entrenamiento y pruebas. En esta técnica es frecuente dividir los datos en 80% para entrenamiento y 20% para pruebas. Esta técnica garantiza la transparencia del modelo, debido a que será evaluado con datos desconocidos.

En RapidMiner, los operadores permiten al usuario llevar a cabo los procesos existentes en el programa, siempre y cuando se establezcan las conexiones correctas, los formatos y los tipos de datos que requieren. Los operadores utilizados para llevar a cabo dichos procesos y generar la síntesis textual se presentan en la Figura 1.

Figura 1

Esquema de operadores para preprocesamiento de datos



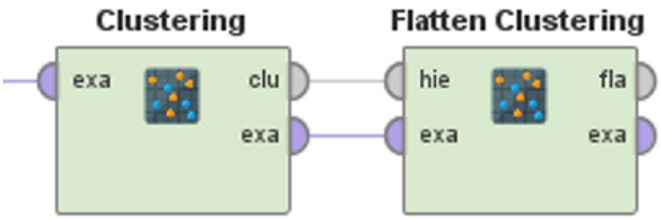
A partir de ahora se pueden aplicar modelos de clasificación o predicción, técnicas de agrupamiento y evaluación. En este estudio se utilizaron dos modelos de árboles de decisión, un modelo estándar, aplicado a partir de los 18 atributos seleccionados, y otro modelo generado a partir de un agrupamiento previo, etiquetando a cada grupo (clúster). En ambos modelos se utilizó el mismo proceso de síntesis previa, donde fueron evaluados y comparados en su tarea de clasificación. El agrupamiento jerárquico aglomerativo (HAC), árboles de decisión y métricas de evaluación fueron los modelos y algoritmos utilizados. Otros modelos, métricas de evaluación y procesos de optimización quedan fuera del alcance de este estudio.

Implementación de la técnica de agrupamiento

Las técnicas de agrupamiento se utilizan con frecuencia en la minería de datos para identificar grupos naturales en los datos a partir de su similitud (Mamani Rodríguez et al., 2017). Existen varios algoritmos de agrupamiento, pero para este estudio se utilizó el HAC debido a su estructura y simplicidad. Este agrupamiento jerárquico considera que cada punto de datos en un grupo individual, luego, en un algoritmo aglomerativo de "abajo hacia arriba" agrupa los puntos hasta formar grupos más grandes mientras sube en su jerarquía (Sharma et al., 2019). Las variables que se utilizaron para implementar la técnica de agrupamiento fueron los 18 atributos seleccionados que componen el cuerpo de la encuesta realizada a los estudiantes universitarios, debido a ser los más relevantes para realizar la síntesis textual. En conjunto, se utilizó un operador adicional que reduce en una sola jerarquía los grupos que se quieren generar, en este caso cuatro grupos. Los operadores que permiten implementar esta técnica se muestran en la Figura 2.

Figura 2

Operadores de agrupamiento



Los parámetros de configuración del operador de agrupamiento se modificaron para trabajar con los datos procesados. El modo o criterio que indica el tipo de enlazar cada punto en el agrupamiento, el tipo de medida indica la medida que se utilizará para medir la distancia entre los puntos, puede ser nominal, numérica o mixta, y a su vez la medida a utilizar. Este parámetro depende del anterior, ya que despliega distintas medidas en función de su tipo. Los parámetros establecidos en RapidMiner se presentan en la Tabla 1.

Tabla 1

Configuración de parámetros del agrupamiento

MODO	ENLACE PROMEDIO
Tipo de medida	Numérica
Medida numérica.	Coeficiente de similitud de Sorensen-Dice

Implementación de árboles de decisión

Los árboles de decisión son un modelo de aprendizaje automático supervisado. Su estructura se compone de nodos, que representan las características o atributos de los datos de entrada, y ramas, que representan las posibilidades de esos atributos (Fletcher e Islam, 2020). RapidMiner ofrece la posibilidad de generar árboles de decisión y modificar algunos de sus parámetros para optimizar su rendimiento.

Asimismo, como en la técnica anterior se utilizaron los 18 atributos preprocesados con la finalidad de obtener resultados más eficientes. Los parámetros que fueron modificados corresponden al criterio, que especifica la forma de selección y división de las ramas, así como la profundidad máxima, que limita el número de ramificaciones. Los valores modificados y el resto de los parámetros se evidencian en la Tabla 2.

Tabla 2

Configuración de parámetros del árbol de decisión

CRITERIO	RELACIÓN DE GANANCIA (GAIN RATIO)
Profundidad máxima	5
Confianza	0.10
Ganancia mínima	0.01
Tamaño mínimo de hojas	2

Evaluación de modelos

Para validar la eficacia de los modelos generados, se utilizaron operadores que permiten evaluar el rendimiento de los modelos a través de varios criterios como la precisión, la exactitud (Accuracy) y la recuperación (Recall). En RapidMiner, previo a la evaluación de los modelos, es necesario un operador que aplique el modelo con los datos de entrenamiento y prueba. Posteriormente, se conecta el operador que mide el rendimiento del modelo. Ambos operadores no disponen de parámetros de configuración.

Finalmente, el rendimiento de los modelos fue evaluado a través de la matriz de confusión generada. De esta manera, fue posible comparar su rendimiento, así como los aciertos y errores en la clasificación de cada modelo, evidenciando cuál presenta las mejores prestaciones. Por consiguiente, los métodos descritos en esta sección son exclusivos de la tarea de síntesis textual sobre el acoso y el ciberacoso.

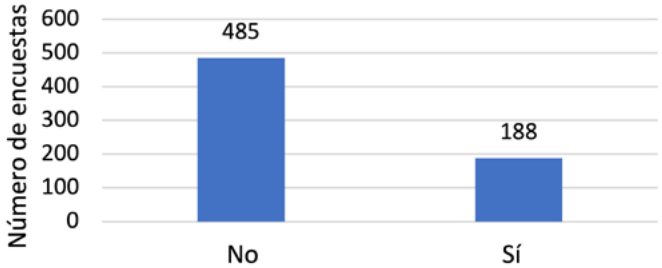
Resultados y Discusión

Los procesos y técnicas de preparación de los datos resultaron en la síntesis textual que se describe a continuación:

- Selección de atributos o variables: se seleccionaron 18 atributos del cuerpo de la encuesta que incluyen datos ordinales (ítems tipo Likert), un identificador (número de encuesta) y un atributo de salida. Este atributo etiqueta al estudiante que ha sufrido de acoso o ciberacoso mediante dos valores (Sí y No).
- Limpieza de datos: al no presentarse más problemas de limpieza de datos, los valores nulos fueron imputados al valor de la media. El número de registros luego de la limpieza se redujo a 673. La Figura 3 muestra la proporción de estudiantes que han sido víctimas de acoso o ciberacoso en la secundaria.

Figura 3

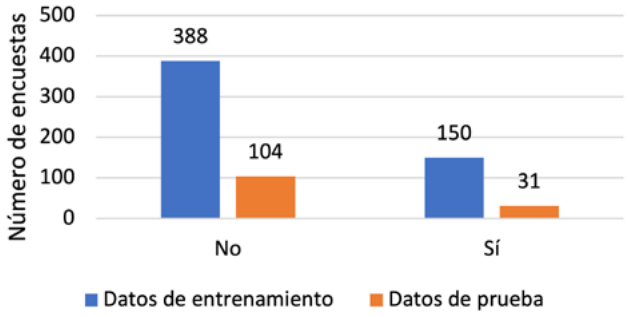
Frecuencia de experiencias con el acoso



- Transformación de los datos: los valores de los atributos o columnas seleccionadas (4. Muchas veces; 3. Bastantes veces; 2. Algunas veces y 1. Nunca) se reemplazaron por dos variables nominales (Sí y No). La división de datos se realizó con un porcentaje de 80% (538 registros) para entrenamiento y 20% (135 registros) para pruebas, como se muestra en la Figura 4.

Figura 4

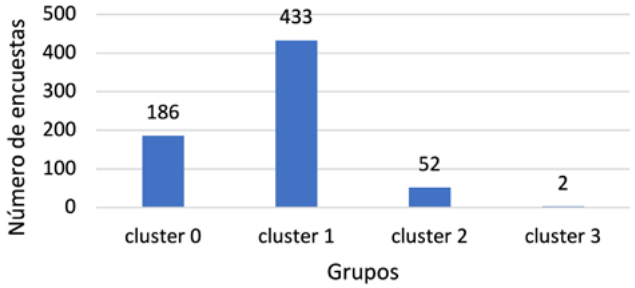
Frecuencia de experiencias en datos de entrenamiento y prueba



- Para el agrupamiento, se transformaron los valores de los registros a un valor numérico (0 y 1), aumentando una columna por cada valor del registro. Esta codificación permitió que el método de agrupamiento jerárquico aglomerativo pudiera procesar y realizar los cálculos numéricos necesarios para el agrupamiento. En la Figura 5 se muestra los cuatro grupos generados en RapidMiner.

Figura 5

Grupos generados



En RapidMiner es posible visualizar los modelos de árboles de decisión a través de gráficos que representan los nodos y ramificaciones del modelo. Aunque en algunas ocasiones, los modelos resultan extensos debido a la cantidad de atributos o su configuración, como ha ocurrido en este caso, por lo que una representación gráfica de los árboles no es adecuada en esta ocasión.

Sin embargo, la matriz de confusión expone el rendimiento del modelo a través de varias métricas, como la precisión para las clases, que indica la proporción de verdaderos positivos sobre el total de calificaciones positivas. Y la métrica de recuperación (Recall) de cada clase, que indica la proporción de verdaderos positivos que se han clasificado correctamente. Esto es realizado a través de la ecuación 1 y 2:

$$precisión = \frac{TP}{TP + FP} \quad (1)$$

$$recuperación = \frac{TP}{TP + FN} \quad (2)$$

Donde *TP* es verdadero positivo, *FP* es falso positivo y *FN* es falso negativo.

El modelo de clasificación sin agrupamiento previo presentó una exactitud del 78.52%, y el modelo de clasificación con agrupamiento presentó una exactitud del 86.57%. En las Tabla 3 y la Tabla 4 exponen la matriz de confusión de ambos modelos, así como los valores de precisión y el porcentaje de recuperación.

Tabla 3

Matriz de confusión del modelo sin agrupamiento

	SI	NO	PRECISIÓN DE LA CLASE
PRED. NO	92	24	79.31%
PRED. SÍ	5	14	73.68%
RECUPERACIÓN DE LA CLASE	94.85%	36.84%	

La precisión de ambas clases de acuerdo con la Tabla 3 es superior al 70%. Por lo tanto, el modelo puede clasificar con precisión al menos esa proporción de registros de estudiantes que sufren de acoso o ciberacoso. Sin embargo, la recuperación de la clase Sí presenta algunas dificultades al modelo, acertando en 14 ocasiones de un total de 38 registros pertenecientes a la clase Sí, dando como resultado una recuperación del 36.84%. Por el contrario, la clase No, que presenta una proporción del 94.85%, acertó en 92 ocasiones de un total de 97 registros de esta clase.

De acuerdo con la Tabla 4, el modelo con agrupamiento previo pudo clasificar a tres de los cuatro grupos formados con una precisión de al menos 75%. Sin embargo, al dividir los datos aleatoriamente en un grupo de entrenamiento y de prueba, no quedaron registros existentes del grupo tres en los datos de prueba. En cuanto a la recuperación, el grupo dos presentó una proporción del 100%, mientras que el grupo uno fue del 97.70%. Lo que acertó en clasificar 85 casos de 87 y finalmente el grupo cero cuya una proporción fue del 56.76%, llegó a clasificar 21 casos correctos de un total de 37 casos pertenecientes a ese grupo.

Tabla 4

Matriz de confusión del modelo con agrupamiento

	CLUSTER 0	CLUSTER 1	CLUSTER 2	CLUSTER 3	PRECISIÓN DE LA CLASE
PRED. CLUSTER 0	21	2	0	0	91.30%
PRED. CLUSTER 1	13	85	0	0	86.73%
PRED. CLUSTER 2	3	0	10	0	76.92%
PRED. CLUSTER 3	0	0	0	0	0.00%
RECUPERACIÓN DE LA CLASE	56.76%	97.70%	100.00%	0.00%	

La síntesis textual facilitó la generación de modelos de clasificación; ambos modelos presentaron una exactitud por encima del 75%. Sin embargo, los resultados evidencian una

mayor exactitud al implementar el modelo con agrupamiento, lo que indica que el proceso de síntesis tuvo una influencia positiva en su rendimiento al predecir los casos correctos de las personas que han sufrido de acoso y ciberacoso. Aun así existen otros factores que pueden alterar los resultados de un modelo de minería de datos, como las tareas de preprocesamiento de datos, la calidad de los datos y el balance de las clases o etiquetas.

Conclusiones

La minería de datos se encuentra en un proceso continuo de avance y transformación, al igual que sus herramientas de software. La generación masiva de información permite la creación de nuevos algoritmos y procesos que permiten analizar y generar conocimiento de cualquier tipo de información, incluso de problemas sociales tan delicados como el acoso y el ciberacoso. Cada día, más jóvenes y adolescentes sufren estos tipos de violencia en sus actividades cotidianas; esto se evidencia en el número de estudiantes universitarios que respondieron afirmativamente a la encuesta sobre sus experiencias con el acoso y el ciberacoso.

Por lo tanto, en este estudio se utilizaron técnicas y algoritmos de minería de datos como árbol de decisión y de agrupamiento a las encuestas aplicadas a los estudiantes universitarios para generar una síntesis textual que permita generar conocimiento sobre el acoso y el ciberacoso. De este modo, al aplicar el modelo de aprendizaje automático supervisado denominado árbol de decisión con los datos obtenidos de las encuestas presentó una exactitud del 78.52%. Sin embargo, al evaluar con los mismos datos sobre el acoso y el ciberacoso, el modelo de clasificación con agrupamiento alcanzó una exactitud del 86.57% al estimar cuando se presentan estos problemas sociales a través de la encuesta realizada. No obstante, es imprescindible realizar tareas de preprocesamiento de datos para lograr un buen desempeño de los modelos, debido a que pueden alterar los resultados del modelo que se está utilizando.

Como trabajos futuros, se plantea el uso de otros modelos de aprendizaje automático y aprendizaje profundo como las redes neuronales; así como otras técnicas de evaluación de modelos como la validación cruzada que pueden ser de utilidad para la generación de conocimiento sobre el acoso y el ciberacoso.

Reconocimientos

Los autores desean agradecer al Vicerrectorado de Investigaciones de la Universidad del Azuay por el apoyo financiero y académico, así como a todo el personal de la escuela de Ingeniería de Ciencias de la Computación, y el Laboratorio de Investigación y Desarrollo en Informática (LIDI).

Referencias

Arce-Ruelas, K. I., Álvarez-Xochihua, O., Pelegrín, L., Cardoza-Avendaño, L., y González-Fraga, J. A. (2022). Automatic Cyberbullying Detection: A Mexican Case in High School and Higher Education Students. *IEEE Latin America Transactions, 20*(5).

Banerjee, V., Telavane, J., Gaikwad, P., y Vartak, P. (2019). Detection of Cyberbullying Using Deep Neural Network. *International Conference on Advanced Computing y Communication Systems (ICACCS)*.

Bozyiğit, A., Bilimleri, B., Dokuz, B., İzmir, E. Ü., Bilgisayar, S. U., Bölümü, M., Eylül, D., İzmir, Ü., Bilgisayar, E. N., y Bölümü, B. (2019). Cyberbullying Detection by Using Artificial Neural Network Models. *International Conference on Computer Science and Engineering (UBMK)*.

Bracco, A. (2018). *Normalización de Texto en Español de Argentina* (pp. 1–68).

Castilla, O. M. N. (2021). Ciberbullying: El acoso escolar en el ciberespacio e implicancias psicológicas. *Hamut'ay, 8*(1), 67–74.

Castro R, L. F., Espitia P, E., y Montilla, A. F. (2018). Applying CRISP-DM in a KDD process for the analysis of student attrition. *Advances in Computing: 13th Colombian Conference, CCC 2018, Cartagena, Colombia, September 26–28, 2018, Proceedings 13*, 386–401.

Cornel, J. A., Pablo, C. C., Marzan, J. A., Mercado, J. V., Fabito, B., Rodriguez, R., Octaviano, M., Oco, N., y la Cruz, A. De. (2019). Cyberbullying Detection for Online Games Chat Logs using Deep Learning. *International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM)*.

Dalvi, R. R., Chavan, S. B., y Halbe, A. (2020). Detecting a Twitter Cyberbullying using Machine Learning. *International Conference on Intelligent Computing and Control Systems (ICICCS)*.

Fletcher, S., y Islam, Md. Z. (2020). Decision Tree Classification with Differential Privacy. *ACM Computing Surveys, 52*(4), 1–33. https://doi.org/10.1145/3337064

Gupta, M. K., y Chandra, P. (2020). A comprehensive survey of data mining. *International Journal of Information Technology, 12*(4), 1243–1257. https://doi.org/10.1007/s41870-020-00427-7

Han, J., Pei, J., y Tong, H. (2022). *Data mining: concepts and techniques*. Morgan kaufmann.

Herrera, C. R. M., Ríos, S. P., y Noboa, I. R. (2018). Indicadores de violencia relacionados con el ciberbullying en adolescentes del Ecuador. *Pensando Psicología, 14*(24).

Jorgensen, S. L., y Siegel, P. B. (2019). *Social Protection in an Era of Increasing Uncertainty and Disruption*. World Bank, Washington, DC. https://doi.org/10.1596/31812

Kathuria, A., Gupta, A., y Singla, R. K. (2021). *A Review of Tools and Techniques for Preprocessing of Textual Data* (pp. 407–422). https://doi.org/10.1007/978-981-15-6876-3_31

Li, C., Wang, P., Martin-Moratinos, M., Bella-Fernández, M., y Blasco-Fontecilla, H. (2022). Traditional bullying and cyberbullying in the digital age and its associated mental health problems in children and adolescents: a meta-analysis. *European Child y Adolescent Psychiatry*, 1–15.

Mahat, M. (2021). Detecting Cyberbullying across Multiple Social Media Platforms Using Deep Learning. 2021 *International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2021*, 299–301. https://doi.org/10.1109/ICACITE51222.2021.9404736

Martin-Criado, J. M., Casas, J. A., Ortega-Ruiz, R., y Rey, R. Del. (2021). Parental supervision and victims of cyberbullying: Influence of the use of social networks and online extimacy. *Revista de Psicodidactica, 26*(2), 161–168. https://doi.org/10.1016/j.psicod.2020.12.005

Mollo, J. P., Larrain, E., y Landazabal, M. G. (2018). Prevalencia de bullying y cyberbullying en Latinoamérica: una revisión. *Revista Iberoamericana de Psicología: Ciencia y Tecnología, 11*(3), 1–18.

Namane, K. C., y Kyobe, M. (2017). Examining the evolution of Mobile Bully - Victims across different schools located in low to high safety risk areas in Cape Town, South Africa. *2017 Conference on information Communication Technology and Society*.

Nielsen, M. B., y Einarsen, S. V. (2018). What we know, what we do not know, and what we should and could have known about workplace bullying: An overview of the literature and agenda for future research. *Aggression and Violent Behavior, 42*, 71–83. https://doi.org/10.1016/j.avb.2018.06.007

Rahman, S., Talukder, K. H., y Mithila, S. K. (2021). An Empirical Study to Detect Cyberbullying with TF-IDF and Machine Learning Algorithms. *Proceedings of International Conference on Electronics, Communications and Information Technology, ICECIT 2021*. https://doi.org/10.1109/ICECIT54077.2021.9641251

Ramirez, A. J. B., y Ccallohuari, H. A. M. (2020). *Modelo de aprendizaje supervisado para pronóstico de la deserción de estudiantes de la Facultad de Ingeniería y Arquitectura de la Universidad Peruana Unión - Lima*.

Roux, M. (2018). A comparative study of divisive and agglomerative hierarchical clustering algorithms. *Journal of Classification, 35*, 345–366.

Ruiz-Chavez, Z., Salvador-Meneses, J., y Garcia-Rodriguez, J. (2018). *Machine Learning Methods Based Preprocessing to Improve Categorical Data Classification* (pp. 297–304). https://doi.org/10.1007/978-3-030-03493-1_32

Schröer, C., Kruse, F., y Gómez, J. M. (2021). A systematic literature review on applying CRISP-DM process model. *Procedia Computer Science, 181*, 526–534.

Shaikh, F. B., Rehman, M., y Amin, A. (2020). Cyberbullying: A Systematic Literature Review to Identify the Factors Impelling University Students towards Cyberbullying. *IEEE Access, 8*, 148031–148051. https://doi.org/10.1109/ACCESS.2020.3015669

Sharma, S., Batra, N., y others. (2019). Comparative study of single linkage, complete linkage, and ward method of agglomerative clustering. *2019 international conference on machine learning, big data, cloud and parallel computing (COMITCon)*, 568–573.

Tapia, F., Aguinaga, C., y Luje, R. (2018). Detection of Behavior Patterns through Social Networks like Twitter, using Data Mining techniques as a method to detect Cyberbullying. *2018 7th International Conference On Software Process Improvement (CIMPS)*, 111–118.