Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN GESTIÓN ECONÓMICA Y FINANCIERA DE RIESGOS

TRABAJO FINAL DE MAESTRÍA

Gestión de riesgos en la CABA: modelos de clasificación para predecir delitos violentos entre 2016 y 2019

AUTORA: MARÍA FLORENCIA AIN

DIRECTOR: JAVIER GARCÍA FRONTI

MAYO 2022

Agradecimientos

A Javier García Fronti, por aceptar dirigir este proyecto. Por su pragmatismo, lucidez, capacidad de asociación y paciencia. Gracias por hacer de la universidad pública un lugar de calidad.

A Gastón, por hacer de mi infancia una etapa muy feliz. A Daniela, por su forma afectuosa y desinteresada de maternarme. A Luciana, por agarrarme siempre fuerte la mano y dedicar cada uno de sus fines de semana a leer y releer lo que escribí, con un amor y una paciencia inconmensurables.

A Rocío, por acompañar y apoyar cada una de mis decisiones, por conocer cosas de mi que ni yo conozco, por enseñarme que el límite es el cielo.

A Nahir, por su forma afectuosa de estar, por su complicidad, por contestarme las mismas preguntas con la misma paciencia.

A Segundo, porque no importa cuán lejos esté, hace que mi mundo sea un lugar mucho más feliz.

A Mario, por compartirme sus anécdotas y confidencias, por hacer de las charlas cotidianas un refugio emocional y mental.

A cada unx de mis sobrinxs, que me llenan de inocencia, frescura y risas.

Resumen

La seguridad pública se encuentra, históricamente, entre las principales inquietudes de los ciudadanos y la comisión de delitos se relaciona directamente con ella. La predicción de delitos está destinada a la anticipación de posibles hechos futuros, tomando como punto de partida el procesamiento y análisis de la información disponible en la actualidad. Incorporar la predicción de delitos al ámbito de la planificación de la política de seguridad constituye un hecho innovador que puede redundar en programas basados en la evidencia y más adecuados a las particularidades de los contextos en que se insertan, con un desarrollo de sistemas de vigilancia y prevención eficaces y adecuados a los recursos disponibles de la jurisdicción. De hecho, según Garland (2005, p. 217), el delito constituye un riesgo que debe ser calculado o un accidente que debe evitarse.

El presente trabajo tiene por objeto predecir la ocurrencia de delitos violentos en la Ciudad Autónoma de Buenos Aires (CABA) a partir de la aplicación de métodos de clasificación a las bases de datos (*datasets*) de delitos publicadas por el Gobierno de la Ciudad de Buenos Aires (GCBA) para encontrar el método de cuantificación de riesgo que mayor exactitud arroje para dicha predicción.

Recién a partir del año 2017, el GCBA publica el conjunto de los datos sobre la criminalidad registrada en el portal BA Data https://data.buenosaires.gob.ar/. Por consiguiente, los datos que se emplean son a partir de enero de 2016 y hasta diciembre de 2019. El criterio de selección de las dimensiones espacio temporales consiste en utilizar los datos disponibles. Cabe mencionar que los delitos cometidos durante el año 2020 no se incorporan al análisis por motivo de la pandemia, la cual ha provocado algunas distorsiones en los valores consignados que afectan cualquier tipo de predicción.

El enfoque del estudio es cuantitativo exploratorio y el tipo de diseño longitudinal. Se realiza un análisis exploratorio de los *datasets* originales de delitos violentos y se procede a la transformación de los atributos del conjunto de datos para mejorar la calidad de las predicciones. A partir de la confección de una única base y su posterior procesamiento en *Rapidminer Studio*, se predice la ocurrencia de delitos violentos utilizando los métodos de aprendizaje supervisado Regresión Logística (RL) y *k* vecinos más cercanos (k-*Nearest Neighbour*, k-NN) para conocer cuál es el que mayor exactitud arroja. Estas herramientas

de cuantificación de riesgo, etapa fundamental dentro de lo que se denomina gestión de riesgo, permiten optimizar la identificación de oportunidades y amenazas, crear un marco para la toma de decisiones informadas, perfeccionar los métodos de seguimiento y monitoreo y mejorar la prevención de hechos delictivos.

Por último, y en base a los resultados obtenidos, se elaboran sugerencias para prevenir el riesgo inherente a la comisión de delitos violentos y/o mitigar su impacto y se plantean futuras líneas de investigación relacionadas con la problemática en cuestión.

Palabras claves: delito violento, gestión de riesgo, *Rapidminer Studio*, predicción.

Clasificación JEL: D81**,** C88, E17

Índice

Introducción

La gestión de la seguridad pública se ha convertido en un eje de política prioritario para los gobiernos en tanto la inseguridad constituye una de las principales preocupaciones de la opinión pública. El delito, como expresión material de la inseguridad, es un fenómeno complejo y multidimensional. En este sentido, las encuestas de victimización, realizadas conjuntamente por el Instituto Nacional de Estadística y Censos (INDEC) y el Ministerio de Seguridad de la Nación, se erigen como un insumo fundamental para comprenderlo y elaborar estrategias de abordaje.

De la última Encuesta Nacional de Victimización (ENV) publicada, se desprende que el 85,1% de la población del país considera la inseguridad en su ciudad de residencia como un problema "bastante o muy grave" (Instituto Nacional de Estadística y Censos [INDEC], 2018, pp. 8-9). Asimismo, resulta destacable que la tasa de no denuncia o "cifra negra" asciende al 66,3% de los delitos contra las personas, porcentaje que en la CABA alcanza al 75,9%, la más elevada del país (Observatorio de Seguridad Ciudadana, s.f.). La desmotivación para no realizar la denuncia puede encontrar justificación en los bajos niveles de confianza que tiene la ciudadanía en las instituciones encargadas de administrar la justicia. Adicionalmente, las políticas de seguridad parecen no contentar a una ciudadanía que al tiempo que descree de la justicia, reclama mayores niveles de punición. Resulta probable que un abordaje más integral del problema del delito reduzca significativamente esta demanda.

El análisis de datos de cualquier índole –en este caso, de seguridad- puede resultar un factor clave para mejorar la administración gubernamental a través de la implementación de políticas públicas basadas en evidencia que satisfagan las necesidades ciudadanas, pero que también resuelvan los problemas que abordan. En este sentido, la predicción de delitos está destinada a la anticipación de posibles hechos futuros, tomando como punto de partida el procesamiento y análisis de la información disponible. Incorporar la predicción de delitos a la planificación de la política de seguridad constituye un hecho innovador que puede redundar en programas más adecuados al contexto en el que se insertan, con datos fiables que pueden ser permanentemente actualizados.

En las últimas décadas, el acceso a datos abiertos y el surgimiento de nuevas tecnologías basadas en internet han posibilitado la difusión de los modelos predictivos como técnicas idóneas para cuantificar los riesgos delictivos. Estos modelos utilizan técnicas propias del aprendizaje automático (*machine learning)* y desarrollan algoritmos que permiten aprender comportamientos de experiencias pasadas (Stamp, 2017). Con la utilización de técnicas analíticas adecuadas se pueden identificar, cuantificar y predecir problemáticas de interés para cualquier gestión de gobierno: a esto se refiere con la denominada "inteligencia de valor público" (Rodríguez et al., 2017, p. 9).

Según Garland, el delito constituye un riesgo que debe ser calculado o un accidente que debe evitarse: las denominadas nuevas criminologías perciben el delito de manera prospectiva y agregada con el objetivo de calcular los riesgos y formular políticas preventivas (2005, p. 217). En este sentido, la gestión o gerenciamiento de riesgos comprende aquellas actividades coordinadas para identificar, analizar, evaluar y clasificar riesgos con el objeto de mitigar sus consecuencias (Organización Internacional de Normalización, 2010). En el presente trabajo, la gestión del riesgo delictivo en la CABA se relaciona principalmente con su cuantificación mediante la predicción de su ocurrencia, utilizando los modelos de clasificación RL y k-NN. Dichos modelos permiten optimizar la identificación de oportunidades y amenazas, crear un marco para la toma de decisiones informadas, perfeccionar los métodos de seguimiento y monitoreo y mejorar la prevención de hechos delictivos.

Los resultados de la aplicación del modelo predictivo más preciso implica una mejora de calidad en la gestión integral de riesgos, contribuyendo al desarrollo de sistemas de vigilancia y prevención de la inseguridad y al diseño de dispositivos de mitigación del impacto de estos hechos en las víctimas; constituyéndose así en una herramienta valiosa también para el uso y la distribución racional de los recursos financieros disponibles, siempre limitados.

Planteamiento del problema

El concepto de seguridad ciudadana está asociado a aspectos objetivos y subjetivos. Dentro del aspecto objetivo, se encuentra el incremento de los delitos y, dentro del subjetivo, el "sentimiento de inseguridad" entendido como esa sensación de incertidumbre permanente y de riesgo potencial con la que los ciudadanos viven ante el aumento de la delincuencia ordinaria o ante el efecto de daño social que genera la repercusión de pocos casos en los medios de comunicación masivos (Behar y Lucilli, 2003).

De hecho, la inseguridad –reducida en general a la percepción de delitos- es un problema fundamental para la mayoría de los argentinos. Por poner un ejemplo, la Encuesta de Satisfacción Política y Opinión Pública (ESPOP) realizada en marzo de 2021 por la Universidad de San Andrés muestra que la inseguridad/robos es uno de los temas que más preocupan a los argentinos, al mismo tiempo que la política de seguridad es la peor evaluada entre todas las áreas de política pública. La falta de políticas claras y eficaces en seguridad contribuye a una sensación de incertidumbre y a un pesimismo social generalizado sobre el empeoramiento del problema, como marcan la mayoría de las encuestas de opinión pública.

Sin embargo, el abordaje del delito no es sólo un problema de las políticas de seguridad. El debate mediático se centra en soluciones unidireccionales y estrictamente punitivas como incrementar las fuerzas policiales o endurecer las leyes que penan los delitos, pero muy poco en la necesidad de una estrategia integral de abordaje de la seguridad, que incluye a la educación como componente esencial (Kessler, 2010).

En términos de Garland (2005, p. 258), la necesidad de la sociedad por sentir que controla los riesgos y las incertidumbres asociadas a la inseguridad involucra campos como la psicología y la sociología del crimen y constituye una cuestión que impacta directamente en la cultura de la clase media.

La posibilidad de predecir la comisión de hechos delictuales puede contribuir al diseño de una política de seguridad que contemple no sólo un sistema de monitoreo y vigilancia de delitos actualizado y adecuado al territorio sino también acciones destinadas a mitigar los

daños que estos delitos generan no sólo en las víctimas, sino también en el entramado social.

Con relación a las bases de datos disponibles para realizar el presente trabajo, existen cuatro tipos de delitos publicados por el GCBA, a saber: homicidios, lesiones, hurtos y robos. No obstante, esta última tipología representa entre el 55% y el 60% de los delitos denunciados durante todo el periodo de estudio. Por su parte, el porcentaje de homicidios sobre el total de delitos denunciados representa menos del 1% y, en el caso de las lesiones, sólo se encuentran publicadas aquellas correspondientes al año 2019. Por dichos motivos, ambos tipos delictivos no se incluyen en la predicción. De esta manera, el análisis se centra en los hurtos, definidos como delitos sin violencia, y en los robos, que constituyen delitos violentos.

Siguiendo esta línea argumental, el objetivo general del presente trabajo consiste en proponer una gestión de riesgos de los delitos violentos en la CABA mediante la predicción de su ocurrencia aplicando los métodos de clasificación RL y k-NN. Para ello, se utilizan las bases de datos de delitos publicadas en el portal BA Data para el periodo comprendido entre los años 2016 y 2019, con el objeto de contribuir al desarrollo de sistemas de vigilancia y prevención de delitos eficaces y adecuados a los recursos disponibles de la jurisdicción.

Con el objeto de operacionalizar el objetivo general, se platean los siguientes objetivos específicos, a saber: trabajar sobre los datos de delitos disponibles en la CABA publicados en el portal BA Data correspondientes a los años 2016, 2017, 2018 y 2019; procesar la base de datos obtenida con el software *Rapidminer Studio* para crear un conjunto de datos óptimos para el análisis predictivo; aplicar los métodos de aprendizaje supervisado RL y k-NN para elegir el modelo que mejor cuantifique los riesgos delictivos en base al resultado de la exactitud de cada uno, y elaborar sugerencias en base a los resultados obtenidos que permiten formular lineamientos para prevenir la comisión de delitos violentos y/o mitigar su impacto.

En concordancia con los objetivos y el tipo de estudio planteado, la hipótesis que sostiene el presente trabajo es que, si se cuenta con una base de datos robusta que contenga información fiable, los métodos de aprendizaje supervisado, RL y k-NN, son las

herramientas más adecuadas para cuantificar los riesgos inherentes a la comisión de delitos violentos y predecir su ocurrencia en un espacio geográfico determinado.

De acuerdo a los objetivos mencionados, el trabajo se estructura de la siguiente manera. En el capítulo 1, se aborda la gestión del riesgo delictivo y la importancia de su predicción para el diseño de políticas de seguridad adecuadas al territorio de aplicación. En el capítulo 2, se detallan las principales técnicas de minería de datos (*data mining*) que se utilizan para gestionar el riesgo haciendo hincapié en la RL y el algoritmo k-NN por ser las más adecuadas para la cuantificación del riesgo y la predicción del delito. En el capítulo 3, se introducen aspectos teóricos sobre el uso y las limitaciones de los datos y los algoritmos, en general, y se analiza esta problemática específicamente en el ámbito del sector público, encargado del diseño de las políticas. En el capítulo 4, se exponen algunos ejemplos sobre predicción de delitos en el ámbito internacional y nacional, y se incluye el mapa del delito de la CABA. En el capítulo 5, se desarrolla la metodología propuesta la cual abarca la selección y el tratamiento de los datos, la aplicación de la RL y el k-NN, la selección de las métricas para evaluar el desempeño de estos modelos y la utilización de la validación cruzada para elegir el más preciso. En el capítulo 6, se exponen los resultados obtenidos y, finalmente, en el capítulo 7 se planten las principales conclusiones y algunas líneas de investigación futuras.

Capítulo 1: Gestión del riesgo del delito y la importancia de su predicción

1.1 Definición de delito

Según el diccionario de la Real Academia Española, un delito es una acción u omisión voluntaria o imprudente penada por la ley. En Argentina, la ley que rige en materia de delitos y su sanción es el Código Penal que en su artículo 164 define el robo como el hecho de apoderarse ilegítimamente de una cosa mueble sea "…con fuerza en las cosas o con violencia o intimidación en las personas, sea que la violencia o la intimidación tengan lugar antes del robo para facilitarlo, en el acto de cometerlo o después de cometido para procurar su impunidad" (Código Penal, 1921, artículo 164). Según nuestro sistema penal, las conductas son consideradas delictivas formal y materialmente cuando, una vez cumplidas todas las etapas procesales, se acredita el comportamiento típico, antijurídico y culpable.

El delito, como expresión material de la inseguridad, es un fenómeno complejo y multidimensional. Las fuentes de información oficiales sobre la ocurrencia de delitos consisten primariamente en los registros administrativos judiciales y policiales. No obstante, dichas fuentes presentan una limitación dado que no incluyen aquellos hechos que no han sido reportados, motivo por el cual no se contemplan en las estadísticas criminales. Siguiendo esta línea argumental, el manual para encuestas de victimización de la Organización de las Naciones Unidas manifiesta que "las fuentes administrativas (…) no pueden ofrecer por sí mismas un análisis suficientemente confiable y exhaustivo." (2010, p. 9).

En el ámbito de la CABA, la Ley N° 2593 del año 2007 crea el Sistema de Información para la Prevención Comunitaria del Delito y la Violencia (SIPREC) que constituye un programa para la prevención del delito y la violencia. Dicha ley fue abrogada por el artículo 524 de la Ley N° 5688 sancionada en el año 2016. Esta última, en su artículo 47, estipula que el mapa del delito, el SIPREC y la encuesta de victimización componen el denominado sistema de gestión de información de seguridad pública. A pesar de que el artículo 67 establece que el resultado de dicha encuesta debe ser publicado en la página

web de la Ciudad, la última y única encuesta disponible en esta materia pertenece al año 2007[1].

En el ámbito nacional, el INDEC y el Ministerio de Seguridad de la Nación realizan conjuntamente las encuestas de victimización que constituyen un insumo fundamental para comprender y elaborar estrategias de abordaje del delito. Se utilizan con el objeto de complementar los datos provenientes de los registros administrativos y recopilan los relevamiento de delitos no denunciados y las razones que conducen a los individuos a no realizar las denuncias. Asimismo, constituyen un diagnóstico para evaluar la relación entre la sociedad y el sistema de seguridad pública.

Al adoptar una definición amplia del concepto de seguridad ciudadana, y como se explicita en la última ENV publicada, las encuestas de victimización "abarcan las representaciones sociales acerca de los delitos y los comportamientos de prevención y autoprotección frente a ellos." (INDEC, 2018, p. 5).

Dicha encuesta analiza ocho ejes estratégicos para abordar el tema de referencia: delitos contra el hogar, delitos contra las personas, denuncias, medidas de seguridad, desempeño del sistema de seguridad pública, percepción de la seguridad ciudadana, victimización y prevalencia delictiva (definida como aquella proporción de hogares o personas que han experimentado uno o más delitos en el período de referencia de la encuesta).

A nivel nacional, una de las características de los delitos contra las personas es que el 78,1% se produjeron en la vía pública (calle, transporte público, plaza o parque y ruta). En el caso de la CABA, esta cifra alcanza el 83,3%, es decir, más del 5% del total a nivel país. Cabe mencionar que la tasa de prevalencia de los delitos violentos (amenaza, agresión física, ofensa sexual y robo con violencia) alcanza un mínimo de 3,1% en Río Negro y un máximo de 14,9% en la provincia de Tucumán. Por su parte, CABA, junto con Salta, Buenos Aires y Santa Fe, superan la tasa nacional y representan el 64% de la población estudiada, motivo por el cual tienen una importancia destacable en la prevalencia total del país (INDEC, 2018, pp. 38 y 27).

[1] Para mayo detalle, https://www.buenosaires.gob.ar/areas/seguridad_justicia/seguridad_urbana/encuesta/.

A este contexto caracterizado por las elevadas tasas de prevalencia de los delitos violentos, se debe agregar la desmotivación de los individuos para no realizar la denuncia. Este hecho puede encontrar justificación en los bajos niveles de confianza que tiene la ciudadanía en las instituciones encargadas de administrar la justicia[2], siendo una creencia que puede tener basamento en diferentes postulados: que determinados delitos menores no justifican el trámite administrativo, que las fuerzas de seguridad locales pueden estar implicadas, algún nivel de involucramiento de la víctima en el hecho, o también temor por parte de la víctima a eventuales represalias (Sozzo, 2008, p. 37). A este fenómeno se lo denomina tasa de no denuncia o "cifra negra" y en Argentina alcanza a un 56,9% de los delitos, mientras que en la CABA asciende a un 64,4%. En el caso de los delitos contra las personas, estas cifran rondan el 66,3% y el 75,9% respectivamente (Observatorio de Seguridad Ciudadana, s.f.).

En cuanto al desempeño del sistema de seguridad pública, la encuesta recaba información acerca del nivel de identificación de las fuerzas de seguridad pública y las instituciones judiciales y su confianza en las mismas. A nivel nacional, el grado de confianza en las instituciones de seguridad y justicia alcanza un 61,9%, con la siguiente composición: 50,8% en las fiscalías, 58,6% en jueces y tribunales y 76,3% en la Policía Federal. Por su parte, en la CABA el nivel de confianza total alcanza un 68,7% conformado según el siguiente detalle: 57% en las fiscalías, 73,2% en jueces y tribunales y 49,9% en la Policía de la Ciudad. Asimismo, en esta jurisdicción, aquellas personas que consideran que el control del delito por parte de la policía provincial es bueno o muy bueno representan el 51,6%, en comparación con Tierra del Fuego que tiene la cifra más alta del país con un 78,9% (Observatorio de Seguridad Ciudadana, s.f).

Con relación a las medidas de seguridad, la ENV recopila datos sobre los cambios en los hábitos y conductas de los ciudadanos producto del miedo a convertirse en víctimas de un hecho delictivo. A nivel país, se puede observar que el 58,4% de los encuestados no permite que sus hijos salgan solos, un 56,4% no lleva mucho dinero en efectivo o tarjetas de crédito y débito y un 43,3% no realiza salidas nocturnas. En el caso de la CABA, el 59,2% no lleva dinero en efectivo o tarjetas (INDEC, 2018, pp. 62-63).

[2] Casi 9 de cada 10 argentinos tienen poca o nada de confianza en la justicia, publicó la ex Ministra de Justicia de la Nación Marcela Losardo en su Twitter el pasado 13 de febrero, según una encuesta telefónica a nivel nacional realizada en enero de 2021. La consultora Isonomía muestra resultados similares (8 de cada 10) en un estudio también telefónico realizado en noviembre de 2020.

En cuanto a la percepción de la seguridad ciudadana, la encuesta intenta medir no sólo los delitos padecidos por las víctimas sino también el riesgo, percibido subjetivamente, de padecerlo. El 41,7% de la población del país considera la inseguridad como un problema muy grave; en la CABA este porcentaje asciende al 54%, el más alto de todo el país (Observatorio de Seguridad Ciudadana, s.f.). Otro indicador utilizado internacionalmente en este tipo de encuestas y que evidencia la percepción de inseguridad lo constituye la proporción de personas que se sienten seguras caminando cerca de sus domicilios. A nivel nacional, sólo el 47,6% de la población admite sentirse segura o muy segura caminando cerca de su lugar de residencia.

1.2 El costo del delito y la desigualdad: una relación proporcional

Ciertas variables socioeconómicas de un país o región se encuentran estrechamente relacionadas con la tasa de delincuencia, a saber: la tasa de desempleo, el Producto Bruto Interno (PBI) per cápita y la distribución del ingreso. Dichas variables explican, en gran parte, la evolución de la tasa del delito. También, se pueden incluir otros indicadores íntimamente relacionados con la distribución del ingreso, como el nivel educativo y las condiciones de acceso al mercado de trabajo (Cerro y Meloni, 1999).

En primer lugar, la tendencia indica que, al aumentar el desempleo, desciende el ingreso proveniente de las actividades legales en comparación con las ilegales, lo que produciría un aumento en la tasa delictiva. En segundo lugar, es factible que las ciudades con mayor PBI per cápita sean más atractivas para delinquir pues presentan mayores oportunidades. En tercer lugar, la desigualdad de ingreso también tiene un efecto positivo en la delincuencia (Cerro y Meloni, 1999).

A fines de los años noventa, los estudios realizados a nivel de países por Bourguignon y Londoño y Guerrero (1999 y 2000, como se citó en Domínguez, 2020, p. 220) evidencian una fuerte relación positiva entre delito violento y desigualdad. La inequidad económica o desigualdad de ingresos está relacionada con la violencia y la criminalidad. Según Dammert (2000), existe una correspondencia entre el incremento de delitos y el incremento de la pobreza y el desempleo, pero principalmente el aumento de la desigualdad.

Desde un punto de vista socioeconómico, el delito es un problema que afecta la calidad de vida de los individuos y el crecimiento económico (Bogomolov et al., 2014, p. 437). Su incremento o disminución depende de diversos factores como la educación, la pobreza, el empleo, la distribución del ingreso y las condiciones socio ambientales (Guerrero Agripino, 2007, p. 257). Asimismo, investigaciones relacionadas con la predicción de delitos sugieren que dichos factores afectan las tasas delictivas (Kim et al., 2018).

Según Kreimer, existen más de 50 estudios que afirman que "la violencia es más común en sociedades en las que hay mayor inequidad, es decir, allí donde hay mayor desigualdad de ingresos y, por tanto, de posibilidades de desarrollo social." (2010, como se citó en Crespo, 2017, p. 66).

En esta línea argumental, el estudio de Fajnzylber et al. (2002, pp. 17-18) utiliza una muestra que involucra alrededor de 40 países y, mediante la aplicación de técnicas estadísticas como el análisis de regresión, se concluye que la desigualdad en el ingreso, medida con el índice de Gini, tiene un efectivo positivo y significativo sobre la incidencia delictiva. Paralelamente, se exponen otros resultados no menos interesantes. Por un lado, la incidencia de los delitos violentos tiene un alto grado de inercia lo que justifica una temprana intervención para prevenir olas delictivas. Por otro lado, las tasas de delitos violentos disminuyen a medida que mejora el crecimiento económico de un país. Finalmente, el nivel medio de ingreso, el nivel educativo promedio de la población adulta y el grado de urbanización no están relacionados de una manera significativa, robusta o consistente con las tasas delictivas.

En todas las investigaciones mencionadas, los países de América Latina presentan esta tendencia que conjuga altas tasas delictivas y una distribución desigual del ingreso, incluso en la actualidad y a nivel subnacional, como señalan Buonanno y Vargas (2019, como se citó en Domínguez, 2020, p. 220). Por consiguiente, el diseño e implementación de políticas que disminuyan la delincuencia y la desigualdad pueden ser mutuamente beneficiosos (Domínguez et al., 2020, p. 233).

La relación entre el crimen y el desarrollo económico y social presenta varias dimensiones. Usualmente, se considera al crimen un gran impedimento para el crecimiento y desarrollo económico y tiende a incrementar la incertidumbre, desalienta las inversiones a largo plazo

y restringe oportunidades de acceso al mercado laboral. Simultáneamente, la falta de crecimiento económico junto con altos niveles de inequidad socioeconómica tiende a aumentar los niveles de violencia y delitos (Naciones Unidas, 2020a, p. 3).

Por lo expuesto, el impacto del delito en el bienestar social y económico de los ciudadanos ha sido objeto de diversas investigaciones: efectos sobre la calidad de vida, costos sociales y costos económicos. Cuantificar el impacto del delito o medir el costo del crimen constituye una tarea difícil pero permite a los gobiernos optimizar la asignación de recursos a intervenciones eficientes que prevengan el delito y mejorar el bienestar de los individuos.

En un estudio realizado sobre 17 países de América Latina y el Caribe, Jaitman y Torre (2017, p. 22) concluyen que el costo promedio de la delincuencia por país para el año 2014 alcanza el 3% del PBI, con una cota inferior y superior del 2,41% y 3,55% respectivamente. En el caso de Argentina, esta cifra se estima en un 2,97% del PIB por año (p. 29).

Para arribar a estas conclusiones, los autores aplican el método de estimación contable que valúa los daños y pérdidas en términos monetarios y luego los suma, comparando escenarios con y sin. Los costos incluidos abarcan: costos sociales del crimen, que incluyen los costos de la victimización en términos de pérdida de la calidad de vida por homicidios y otros delitos violentos y el lucro cesante de la población penitenciaria; costos incurridos por el sector privado, que contemplan el gasto de las empresas y los hogares en servicios de seguridad; y costos incurridos por el gobierno, compuestos por el gasto público en el sistema judicial, la prestación de servicios policiales y la administración de prisiones (Jaitman y Torre, 2017, p. 22).

Asimismo, las estimaciones arrojan que los costos de seguridad ciudadana del gobierno constituyen el principal componente del costo del crimen y ascienden, en promedio, al 1,51% del PBI (Jaitman y Torre, 2017, p. 27). Por lo expuesto, se puede deducir que los costos del crimen pueden ser elevados “no necesariamente por el delito mismo, sino porque la respuesta del gobierno al crimen es subóptima.” (Jaitman y Keefer, 2017, p. 5).

Silva Lira (2000) aborda el concepto de la seguridad ciudadana mediante un análisis costo-beneficio para calcular el costo económico de los delitos en las comunas del Gran Santiago, así como los niveles de vigilancia policial que se requieren en las mismas. Para ello, propone la estimación de un indicador de productividad policial que permita justificar los costos de inversión relacionados con el aumento de los niveles de vigilancia policial (p. 24). No obstante, el nivel de delincuencia se plantea no sólo en función del nivel de vigilancia sino también de otras variables socioeconómicas como el medio ambiente familiar, el nivel de desocupación y el nivel de educación formal, entre otras (p. 38). Por lo tanto, si la reducción del nivel de delitos redunda en beneficios sociales que superen los costos de inversión, resulta plausible justificar las acciones de vigilancia.

1.3. Seguridad pública, prevención y predicción del delito

El concepto de seguridad pública tiene múltiples acepciones, por ello, resulta necesario delimitarlo. En CABA, la Ley N° 5688 del Sistema Integral de Seguridad Pública sancionada en el año 2016 la define como aquella situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías.

En el año 2015, los estados miembros de la Organización de las Naciones Unidas (ONU) adoptan los 17 Objetivos de Desarrollo Sostenible (ODS) con el compromiso de erradicar la pobreza en todas sus formas y dimensiones, luchar contra la desigualdad dentro y entre los países, fomentar la inclusión social, entre otros. Por su parte, el objetivo 16 denominado “Paz, justicia e instituciones sólidas” tiene por objeto reducir todas las formas de violencia mediante el trabajo conjunto con los gobiernos y la sociedad civil para hallar soluciones de largo plazo al problema de la inseguridad. Entre sus metas, se encuentra la de disminuir todas las formas de violencia y las tasas de mortalidad asociadas.

En las últimas décadas, la gestión de la seguridad pública se ha convertido en un eje de política prioritario para los gobiernos en tanto el problema de la inseguridad se ha convertido en uno de los temas centrales de las preocupaciones de la opinión pública (Beltrame, 2013). La mayoría de las encuestas de opinión pública señalan que la ausencia

de políticas de seguridad claras contribuye a una sensación de incertidumbre y a un pesimismo sobre el empeoramiento del problema del delito.

La inseguridad es un problema fundamental para la mayoría de los argentinos. Por poner un ejemplo, la última ESPOP realizada en marzo de 2021 por la Universidad de San Andrés muestra que la inseguridad/robos es uno de los temas que más preocupan a los argentinos, al mismo tiempo que la política de seguridad es la peor evaluada entre todas las áreas de política pública[3].

El abordaje del delito no es sólo un problema de las políticas de seguridad, el debate mediático se centra en soluciones unidireccionales como incrementar las fuerzas policiales o endurecer las leyes que penan los delitos, pero muy poco en la necesidad de una estrategia integral de abordaje de la seguridad, que incluye a la educación como componente esencial (Kessler, 2010).

La cuestión de la "inseguridad" se reduce alrededor del delito "común", es decir, delitos contra la propiedad y las personas mediante el uso de violencia (Ayos, 2014, p. 177). En este sentido, ciertos delitos no tienen vinculación con lo que socialmente se define como "inseguridad", como el caso de los homicidios por siniestro vial o los denominados delitos "de guante blanco" (Lorenc Valcarce, 2013, p. 28).

El concepto de seguridad ciudadana está asociado a aspectos objetivos y subjetivos (Sozzo, 2008, p. 59). Dentro del aspecto objetivo, se encuentra el incremento de los delitos y, dentro del subjetivo, el "sentimiento de inseguridad" entendido como esa sensación de incertidumbre permanente y de riesgo potencial con la que los ciudadanos viven ante el incremento de la delincuencia ordinaria o ante el efecto de daño social que genera la repercusión de pocos casos en los medios de comunicación masivos (Behar y Lucilli, 2003, p.3). Como sugiere Guerrero Agripino (2007), la implementación de programas y políticas de seguridad no sólo debe evitar la ocurrencia de delitos sino también "promover en la ciudadanía la certeza de que eventos de este tipo serán lejanos y no inminentes." (p. 258).

[3] La inseguridad es el primer problema mencionado por el 43% de la gente mientras que el nivel de insatisfacción con la política de seguridad alcanza un 87%.

Como señala Kessler (2009), durante los últimos años se puede advertir el fracaso del denominado modelo tradicional de tratamiento del delito, relacionado con la represión y el mantenimiento del orden social mediante medidas reactivas. En su lugar, las políticas públicas de seguridad han puesto el énfasis en la prevención vinculada a determinado tipos de delito -contra las personas y la propiedad- considerados como productos de la "nueva delincuencia" y causa primaria de la inseguridad social. La crisis de legitimidad de las instituciones policiales, el aumento del mercado privado de seguridad y las limitaciones de las políticas públicas para solucionar el problema, colocan a la delincuencia en una posición clave en las agendas política y estatal y en el centro del debate público (Beltrame 2013, p. 202).

En el marco del incremento sostenido de las tasas de delitos y la elevada sensación de inseguridad, la prevención del delito depende, en gran parte, de los hacedores de políticas (Naciones Unidas, 2020b) que deben contemplar todos los factores causales que atraviesan la problemática. Como afirman Dammert y Arias (2007), existen características específicas que deben incluirse en la estrategia de seguridad pública a pesar de que los resultados se observen en el mediano y en el largo plazo. En este sentido, para Sherman (1998, como se citó en Dammert y Arias, 2007, p. 47) la prevención del delito impacta en las conductas futuras de los individuos.

La tasa de no denuncia o "cifra negra" del delito requiere un abordaje diferencial por parte de los encargados de diseñar e implementar políticas públicas, con el objeto de fortalecer la seguridad ciudadana y los sistemas que imparten justicia. Aquellos hechos delictivos que no son reportados quedan "invisibilizados" para los organismos estatales responsables de prevenirlos y, además, no se pueden predecir. Para comprender el delito de manera multidimensional, resulta necesario considerar no sólo la cantidad de denuncias realizadas sino también aquellas que no se hayan realizado (Flores-Gutiérrez, 2021, p. 44).

Adicionalmente, diversas investigaciones indican que el gasto en prevención del delito es más eficiente que aquel que se destina a implementar medidas de represión. Una mejora en la eficacia policial y un buen funcionamiento del sistema judicial pueden influir no solamente en la disminución del delito sino que también contribuyen a mejorar la percepción de seguridad de los ciudadanos y su confianza en las instituciones (Dammert y Arias, 2017).

Para abordar un fenómeno tan complejo y dinámico como la delincuencia, es menester contar con datos fiables que permitan construir estadísticas oficiales de calidad. Resulta fundamental disponer de distintas fuentes de información, incluidas las encuestas de victimización, que permitan recolectar datos periódicamente y en tiempo real para realizar estudios comparativos a nivel nacional y subnacional (Dammert, 2000, p. 7). En aquellos países donde los niveles de institucionalidad del estado es débil, las estadísticas suelen ser poco confiables por diversos motivos como la falta de rigurosidad en los datos, la alta tasa de no denuncia, la falta de procesamiento y sistematización de la información y el poco uso de tecnologías de la información (Dammert y Arias, 2007).

En esta misma línea argumental, Domínguez (2020, p. 233) señala que en América Latina no hay un conocimiento acabado sobre el "desempeño real de las instituciones de justicia y otros organismos de seguridad como la policía". La información disponible sobre el control del delito y la administración de justicia es escasa. Por ello, resulta indispensable disponer de datos robustos y confiables que permitan diseñar políticas en materia de seguridad y equidad distributiva que apunten a disminuir las tasas delictivas, mejorar la distribución del ingreso y asignar los recursos públicos (incluyendo las fuerzas policiales) de manera eficiente.

En el proceso de toma de decisiones, la disponibilidad y calidad de la información permite realizar un diagnóstico riguroso de la problemática y contrarrestar el efecto de criterios subjetivos relacionados a la discrecionalidad política, los medios de comunicación y la percepción de la inseguridad (Chinchilla y Vorndran, 2018). A efectos de anticipar estrategias que contribuyan a contener y neutralizar el delito, es necesario construir modelos predictivos para pronosticar tendencias y patrones que contribuyan a una gestión preventiva del riesgo.

La criminología moderna, caracterizada por los rasgos de un estado social y democrático de derecho, aborda el fenómeno delictivo como un problema social. No importa la represión del delito y el mantenimiento del orden social a través de acciones reactivas, sino su prevención y la generación de políticas de anticipación y capacidad en la gestión del conflicto. En este sentido, la predicción de delitos resulta de relevancia para la política pública en materia de seguridad.

El análisis predictivo tiene por objeto optimizar el uso de las bases de datos para anticipar eventos delictivos (Rummens et al., 2017), es decir, determinar la probabilidad de ocurrencia de hechos futuros, a partir del procesamiento y estudio de la información actual e histórica. Incorporar dicho análisis a la planificación de políticas de seguridad puede redundar en programas más adecuados al contexto en el que se insertan, con datos fiables que pueden ser permanentemente actualizados.

La predicción del crimen consiste en un enfoque sistemático para encontrar patrones criminales y tendencias a partir del procesamiento de las bases de datos que contienen los delitos denunciados. Para ello, resulta necesario estudiar los factores y relaciones entre los distintos tipos de crimen y encontrar una predicción adecuada que permita evitarlos (Varshitha et al., 2017). Es en este sentido que puede contribuir al diseño de una política de seguridad que contemple no sólo un sistema de monitoreo y vigilancia de delitos actualizado y adecuado al territorio, sino también acciones destinadas a mitigar los daños que estos delitos generan no sólo en las víctimas, sino también en el entramado social.

Como sostienen Rummens et al. (2017), existe una doble perspectiva de abordaje de la vigilancia policial: por un lado, brindar predicciones óptimas del riesgo delictivo y, por otro, determinar estrategias que hagan eficiente el uso de dichas predicciones. No sólo resulta fundamental combinar la dimensión analítica y práctica de la vigilancia policial predictiva sino también determinar si los departamentos de policía pueden utilizar esta información y de qué manera. Si las predicciones no pueden traducirse en acciones concretas para reducir las tasas de delitos, poco puede esperarse de la capacidad anticipatoria de la policía para prevenir los hechos delictuales.

La gran cantidad de información circulante y las múltiples variables que intervienen para predecir la ocurrencia de los delitos, justifica la utilización de herramientas más potentes que los métodos estadísticos convencionales con el objeto de determinar relaciones multivariantes subyacentes (Jha, Jha et al., 2019). En este sentido, la minería de datos así como el descubrimiento de conocimientos en los datos, el aprendizaje automático, la visualización de datos y la teoría de bases de datos, permite cuantificar el riesgo en grandes volúmenes de datos y realizar un análisis predictivo de la ocurrencia de delitos con el objeto de establecer políticas de inteligencia criminal.

En el siguiente capítulo, se exploran las técnicas relacionadas con el aprendizaje automático supervisado y no supervisado como herramientas de cuantificación de riesgos con el objeto de encontrar el modelo que permita predecir los delitos violentos de manera más precisa para, posteriormente, diseñar una gestión preventiva del delito basada en evidencia.

Capítulo 2: La gestión del riesgo delictivo con minería de datos

2.1 Gestión del riesgo delictivo: definición y objetivo

Existen múltiples definiciones y tipos de riesgo. Según la Real Academia Española, la palabra riesgo tiene dos acepciones: por un lado, se lo define como una contingencia o proximidad de un daño y, por otro, como cada una de las contingencias que son pasibles de un contrato de seguro. En otras palabras, el riesgo puede definirse como la probabilidad de ocurrencia de un evento desfavorable y sus consecuencias inherentes. Esta conceptualización permite distinguir no sólo la probabilidad de ocurrencia en sí misma, relacionada indefectiblemente al concepto de incertidumbre, sino también la pérdida asociada a dicha ocurrencia (Dorofee et al., 1996, p. 20). En este sentido, la gestión o gerenciamiento de riesgos comprende aquellas actividades coordinadas para identificar, analizar, evaluar y clasificar los riesgos con el objeto de mitigar sus consecuencias (Organización Internacional de Normalización, 2010).

Según Garland (2005), el delito constituye un riesgo que debe ser calculado o un accidente que debe evitarse. Este enfoque se encuadra dentro de las denominadas "nuevas criminologías de la vida cotidiana", que el autor define como un "conjunto de marcos teóricos afines que incluyen la teoría de las actividades rutinarias, del delito como oportunidad, del análisis de los estilos de vida, de la prevención situacional del delito y ciertas versiones de la teoría de la elección racional." (p. 217). A partir de este marco teórico, el delito se percibe de manera prospectiva y agregada con el objetivo de calcular los riesgos y formular políticas preventivas.

En este marco, la gestión de riesgos abarca las iniciativas coordinadas para identificar, analizar, calcular y clasificar los delitos con el objeto de predecir hechos delictivos que permitan implementar políticas preventivas en materia de seguridad. Este proceso también incluye el análisis de datos como parte de una gestión integral de riesgos por parte del estado. Si bien éste puede transferir una parte del riesgo delictivo a otras entidades (sean empresas de seguridad privada u organizaciones vecinales), es su obligación gestionarlo, siendo los modelos predictivos los instrumentos más eficaces para intentar disminuir la probabilidad de ocurrencia de delitos violentos.

Para predecir delitos, se utilizan técnicas del aprendizaje automático que usan métodos estadísticos y desarrollan algoritmos que permiten aprender comportamientos de experiencias pasadas (Stamp, 2017). En las últimas décadas, el acceso a datos abiertos y el surgimiento de nuevas tecnologías basadas en internet han posibilitado la difusión de los modelos predictivos como técnicas idóneas para cuantificar los riesgos delictivos.

Las técnicas propias del aprendizaje automático brindan sistemas de medición de riesgos más precisos y personalizados en función de las demandas de cada organización que les permiten crear una estrategia de gestión de riesgos integral. Al evitar utilizar hipótesis previas para la creación de modelos, como lo hace la estadística clásica, permite descubrir patrones y tendencias ocultos en los conjuntos de datos que redundan en modelos con mayor poder predictivo.

Los beneficios inherentes a la utilización y análisis de datos por parte de las organizaciones resultan innegables: contribuyen en la predicción, anticipación y minimización de los riesgos vinculados a su operatoria específica. La existencia de grandes volúmenes de datos requiere de modelos propios del aprendizaje automático que permitan procesarlos, lo que genera una mejora significativa de las capacidades analíticas en gestión de riesgos. Al basarse en un aprendizaje continuo y automático, disminuye el margen de error y evalúa permanentemente patrones y desvíos de manera más eficiente que las herramientas estadísticas tradicionales.

En el presente trabajo, se aborda la gestión de riesgo delictivo desde su cuantificación. A partir del cálculo de la probabilidad de ocurrencia de delitos violentos, la aplicación de los modelos de clasificación RL y k-NN permite optimizar la identificación de oportunidades y amenazas, crear un marco para la toma de decisiones informadas, perfeccionar los métodos de seguimiento y monitoreo y mejorar la prevención de hechos delictivos.

Los resultados de la aplicación del modelo más preciso de predicción de ocurrencia de delitos violentos pueden contribuir al desarrollo de sistemas de vigilancia y prevención de la inseguridad y al diseño de dispositivos de mitigación del impacto de estos hechos en las víctimas; constituyéndose así en una herramienta valiosa también para el uso y distribución racional de los recursos financieros disponibles, siempre limitados.

2.2 Minería de datos y aprendizaje automático

Los métodos estadísticos se utilizan generalmente para caracterizar globalmente una clase de objetos (una tabla de datos), pero no para determinar una descripción que prediga clases de objetos futuros (Perichinsky et al., 2000).

La minería de datos consiste en encontrar patrones útiles en los datos (Han et al., 2012, p. 8) y sus técnicas son empleadas no sólo para predecir el delito. Se utilizan en las ciencias médicas para detectar de manera temprana enfermedades basándose en las historias clínicas o predecir brotes epidémicos, en educación, para predecir el rendimiento de los estudiantes o detectar potenciales casos de abandono; en banca y finanzas, para detectar fraudes en las tarjetas de crédito o descubrir correlaciones de ciertos indicadores financieros; en seguros, para predecir qué clientes pueden adquirir nuevas pólizas e identificar perfiles de riesgo en la cartera de clientes; en ventas y el marketing, para analizar qué productos se adquieren simultáneamente en una determinada cesta de compra y/o predecir el comportamiento de los consumidores, entre otras disciplinas (Pitropakis et al., 2019, p. 1; Shojaee et al., 2013, p. 369; Han et al., 2012, pp. 607-618; Naik et al., 2020).

La minería de datos es un procedimiento para analizar datos a partir de un conjunto de información que permita transformarlo en una estructura adecuada para una utilización adicional. Asimismo, predice patrones futuros y permite a las organizaciones tomar decisiones a partir del aprendizaje (Prabakaran y Mitra, 2018, p. 1; Cheng, Chung et al., 2003). También refiere al descubrimiento de conocimiento, aprendizaje automático y análisis predictivo. No obstante, cada uno de estos términos tiene connotaciones ligeramente diferentes dependiendo del contexto en el cual se utilice (Kotu y Deshpande, 2015, p. 2).

Asimismo, utiliza métodos computacionales especializados para descubrir estructuras significativas y útiles en los datos. Dichos métodos derivan de la estadística inferencial, el aprendizaje automático y la inteligencia artificial (Valenga et al., 2007). Asimismo, coexiste y está íntimamente relacionada con áreas conexas tales como los sistemas de bases de datos, la limpieza y visualización de los mismos, el análisis exploratorio de los datos y la evaluación de resultados (Kotu y Deshpande, 2015, p. 3).

El descubrimiento de conocimiento en las bases de datos es el proceso no trivial de identificar relaciones o patrones válidos, novedosos, útiles y comprensibles en los datos para tomar decisiones (Fayyad et al., 1996). El término "proceso no trivial" diferencia a la minería de datos de los cálculos estadísticos, como calcular el promedio o el desvío estándar. La minería de datos involucra la inferencia e iteración de diferentes hipótesis. Uno de sus aspectos claves es el proceso de generalización de patrones a partir de una base de datos. Esta generalización debería ser válida no sólo para el conjunto de datos usado para observar ese patrón sino también para los nuevos datos desconocidos. El término "novedoso" indica que la minería de datos usualmente está asociada a encontrar previamente patrones desconocidos en los datos. El objetivo último de esta disciplina consiste en encontrar conclusiones potencialmente útiles que puedan ser aplicadas por los usuarios (Kotu y Deshpande, 2015, p. 3).

También se puede definir la minería de datos como el proceso de descubrir previamente patrones desconocidos en los datos usando métodos automáticos iterativos. Los algoritmos son procedimientos iterativos que transforman las variables de entrada (*inputs)* en una o más variables de salida (*outputs)*. La aplicación de algoritmos sofisticados para extraer patrones útiles de los datos es lo que diferencia a la minería de datos de las técnicas tradicionales de análisis de datos. Dichos algoritmos automatizan el proceso de búsqueda de una solución óptima para un problema de los datos dado. Basándose en el problema de los datos, esta disciplina se clasifica en tareas tales como la clasificación, el análisis de asociación, el agrupamiento (*clustering)* y la regresión. Cada una de estas tareas usa algoritmos específicos como los árboles de decisión, las redes neuronales, los k-NN y las k-medias (*k-means*), entre otros modelos (Kotu y Deshpande, 2015, pp. 4-5).

Como afirman Fayyad y Uthurusamy (2002, como se citó en Chen et al., 2004, p. 50), la minería de datos es una herramienta poderosa que permite a los investigadores explorar grandes bases de datos de manera rápida y eficiente. Entender la relación entre la capacidad de análisis y las características de los tipos de crimen puede ayudar a los investigadores a utilizar de manera más eficiente estas técnicas para abordar integralmente este tipo de problemáticas, identificar tendencias y patrones e incluso predecir los delitos (Chen et al., 2004, p. 52).

Por otro lado, el aprendizaje automático, según Michalski et al. (1998, como se citó en Servente, 2002, p. 5) es el campo dedicado al desarrollo de métodos computacionales para los procesos de aprendizaje, y a la aplicación de los sistemas informáticos de aprendizaje a problemas prácticos. Se crea, a partir de una necesidad humana, como un desarrollo tecnológico para analizar grandes volúmenes de datos (Meiliana et al., 2020; Dey, 2016). Emplea algoritmos recursivos que permiten encontrar la mejor predicción de un *output* a partir de variables de entrada y que "aprenden" de los errores predictivos de experiencias anteriores (Kotu y Deshpande, 2015).

Según Sammut y Webb (2011, como se citó en Pérez Verona y Arco García, 2016, p. 44) constituye la parte de la inteligencia artificial que comprende el aprendizaje a partir de experiencia pasada (Talaviya et al., 2020; Jha, Doshi et al., 2019; Musumeci et al., 2018) y permite abordar problemas de clasificación, asociación, agrupamiento, y selección de rasgos (Gupta et al., 2020). Recientemente, ha sido aplicado en diversas áreas de investigación como los vehículos autónomos o robóticos, el reconocimiento de voz, la búsqueda web y el mejor entendimiento del genoma humano (Kim et al., 2018; Dey, 2016; Musumeci et al, 2018).

Cabe destacar que la bibliografía disponible sobre minería de datos y aprendizaje automático es tan extensa que resulta difícil abarcar todas las técnicas que se utilizan (Musumeci et al., 2018, p. 1384). No obstante, se brinda una visión global de los principales algoritmos aplicados en distintas áreas de estudio y, particularmente, en la predicción del delito.

2.3 Aprendizaje supervisado o predictivo y aprendizaje no supervisado o descriptivo

Un modelo o clasificador es una representación entre las variables que son dadas, denominadas independiente, y las que se quieren predecir, llamadas variables dependientes (García Cambronero y Gómez Moreno, 2006). La construcción de un modelo, en el marco del aprendizaje automático, puede realizarse utilizando técnicas propias del aprendizaje supervisado o predictivo, o bien, del no supervisado o descriptivo (Kotu y Deshpande, 2015, p. 3; Dey, 2016; Musumeci et al, 2018).

El objetivo de los diferentes métodos de aprendizaje supervisado consiste en construir una función de mapeo y = f(X) que permite predecir el valor de la variable de salida *y*, de acuerdo a los valores de las variables de entrada *x* (Musumeci et al., 2018). Los *inputs* se conforman por las variables independientes o predictoras, mientras que el *output* o variable dependiente constituye la variable de predicción. El aprendizaje se realiza a través de la aplicación de un algoritmo en un conjunto de datos de entrenamiento, que posteriormente se prueba en un conjunto de datos desconocidos para obtener la predicción de la variable objetivo (Arshad Zaidi et al., 2018, p. 236; Han et al., 2012, p. 330).

A su vez, los modelos utilizados por el aprendizaje supervisado pueden dividirse en dos categorías: paramétricos, en los cuales el número de parámetros es fijo; y no paramétricos, donde dicho número depende del conjunto de entrenamiento (Musumeci et al., 2018).

Por un lado, en los modelos paramétricos la función *y* es una combinación de un número fijo de funciones de bases paramétricas. El conjunto de entrenamiento se emplea para estimar un conjunto fijo de parámetros que, luego de la etapa de aprendizaje, se utilizan para realizar la predicción. Ejemplos de este tipo son los modelos lineales de regresión y clasificación (Musumeci et al., 2018).

Por otro lado, los modelos no paramétricos utilizan para la predicción un subconjunto o la totalidad del conjunto de entrenamiento, dado que no están sujetos a ninguna relación funcional. Los enfoques más conocidos son el algoritmo k-NN y las máquinas de soporte vectorial (*Support Vector Machines*, SVM), que pueden aplicarse tanto para tareas de regresión como de clasificación (Musumeci et al. 2018).

Los métodos de aprendizaje supervisado permiten resolver problemas de regresión o clasificación, dependiendo de si la variable objetivo es continua o discreta (Musumeci et al., 2018). La clasificación permite extraer información significativa a partir de grandes conjuntos de datos y puede utilizarse para predecir clases desconocidas (Shojaee et al., 2013, p. 364; Wahbeh et al., 2011, p. 62). En otros términos, se clasifica un conjunto de objetos con propiedades en común en diversas clases, utilizando un conjunto de entrenamiento con ciertos atributos y el valor de la clase a la que corresponde para construir el modelo (Chen et al., 1996; Han et al., 2012, pp. 328-329).

En este sentido, el punto de partida de cualquier modelo de clasificación es la elección de las variables de entrada (Sayeh y Bellier, 2014, p. 3). Resulta de vital importancia no sólo elegir aquellos atributos que brinden la mayor información dentro del conjunto de datos sino también no descartar información crítica para la clasificación (Iqbal et al., 2013, p. 2).

En el contexto del análisis predictivo, un modelo de clasificación tiene por objeto predecir una variable objetivo, sea binaria o categórica, dado un conjunto de variables de entrada. Dicho modelo "aprende" la relación entre la variable que se quiere predecir y los atributos de entrada para un conjunto de datos de entrenamiento dado. Asimismo, esta relación depende del algoritmo elegido para corroborar o refutar la hipótesis planteada (Kotu y Deshpande, 2015, p. 13), entre los cuales cabe mencionar las reglas de inducción, los árboles de decisión, los bosques aleatorios (*Random Forest*), los modelos bayesianos, las redes neuronales, las SVM, los k-NN, la Regresión Lineal y la RL.

En el caso de las reglas de inducción, las mismas permiten deducir, utilizando *datasets* o árboles de decisión, reglas del tipo "si-entonces" que exponen la relación entre las etiquetas y los atributos.

Por su parte, los árboles de decisión abordan el problema de la clasificación mediante la partición de los datos en subconjuntos más "puros" basándose en los valores de los atributos de entrada. Estos subconjuntos influyen significativamente en la variable objetivo y se posicionan en la raíz del árbol o cercanos a ésta. Dicho árbol permite predecir nuevos datos no etiquetados (Kotu y Deshpande, 2015, p. 13). A medida que aumenta la profundidad del árbol, las reglas de decisión se tornan más complejas y ajustan mejor al modelo. Como afirman Curram y Mingers (1994, como se citó en Arshad Zaidi et al., 2018, p. 242), este algoritmo produce reglas lógicas fáciles de interpretar pero tiende a ser susceptible al ruido.

Los bosques aleatorios también abordan problemas de clasificación y están constituidos por un conjunto de árboles de decisión, cada uno de los cuales emplea una muestra diferente del conjunto de datos de entrenamiento que se obtiene mediante técnicas de remuestreo (Kotu y Deshpande, 2015, p. 160). De este modo, las predicciones de todos los árboles individuales se agregan para obtener la predicción de un nuevo dato no etiquetado.

Los clasificadores bayesianos (*Naïve Bayes)* calculan la probabilidad para cada valor de la variable de clase, dados los valores de las variables de entrada. Utilizando las probabilidades condicionales para un registro desconocido, computan los resultados de todos los valores de las clases objetivo y predicen un ganador (Kotu y Deshpande, 2015, p. 13).

Con relación a las redes neuronales, éstas constituyen un modelo conformado por nodos interconectados que transmiten señales e información entre sí que procesan y generan predicciones para encontrar soluciones al problema originalmente planteado. Además, tiene la ventaja de manejar eficientemente relaciones no lineales entre las variables de entrada y la de salida debido al uso de funciones de activación (Arshad Zaidi et al., 2018, p. 239).

En el caso de las SVM, abordan problemas de reconocimiento óptico de caracteres, es decir, detectan límites entre diferentes patrones para poder identificar caracteres. De esta manera, el algoritmo puede identificar si una muestra de datos determinada pertenece a una clase en particular o está fuera de ella (Kotu y Deshpande, 2015, p. 14).

El algoritmo k-NN es un método no paramétrico que asume que *inputs* similares tienen *outputs* similares, es decir, no existe ninguna hipótesis acerca de la distribución subyacente en los datos (*lazy learning)*. El valor de *k* indica el número de registros de entrenamiento cercanos que deben considerarse al hacer la predicción para un registro de prueba sin etiqueta, es decir, indica el número de vecinos considerados para hacer la predicción. Se le suele asignar un valor impar para un problema de dos clases dado que la clase del registro objetivo se evalúa mediante votación (Kotu y Deshpande, 2015, p. 101). Cada nuevo ejemplo lo clasifica calculando la distancia del mismo con todos los ejemplos del conjunto de entrenamiento. Para ello, se necesita especificar una métrica adecuada para medir la proximidad que, en el presente trabajo, es la distancia euclidiana.

La Regresión Lineal tiene por objeto representar la relación entre la variable objetivo o dependiente y las variables independientes, las cuales deben ser todas numéricas. Por su parte, la RL predice una variable objetivo que puede ser binomial o categórica utilizando los atributos como predictores, los cuales deben ser numéricos (Kotu y Deshpande, 2015,

p. 14). En el presente trabajo, la variable binaria o binomial a predecir es delito violento y no violento, a partir del uso de atributos numéricos.

Para predecir patrones delictivos, el uso de aprendizaje automático debe basarse en la elección del algoritmo adecuado para generar las predicciones más exactas posibles (Meiliana et al., 2020). Según la bibliografía vinculada a esta temática, la RL y el algoritmo k-NN son modelos que arrojan una exactitud deseable respecto a la predicción. La RL se ha convertido en una de las herramientas de análisis más utilizadas para las investigaciones sobre la delincuencia y la justicia (Weisburd y Britt, 2014, p. 549).

Por otra parte, los métodos de aprendizaje no supervisado descubren patrones y tendencias en los datos actuales, es decir, no se conoce a priori ningún valor objetivo para predecir. A partir de las variables de entrada, aprenden la estructura subyacente de los datos a través de patrones ocultos, asociaciones y similitudes sin un *output* conocido (Arshad Zaidi et al., 2018, p. 244; Simon et al., 2016). El sistema observa los ejemplos que recibe y busca características en común para formar grupos. Estos métodos generan "un conjunto de descripciones de clases, que juntas cubren todas las clases y en particular describen a una única clase" (Servente, 2002, p. 12). Asimismo, permiten resolver problemas de asociación, agrupamiento y detección de anomalías.

Por su parte, una regla de asociación implica el descubrimiento de relaciones de asociación o correlación en un conjunto de datos (Kotu y Deshpande, 2015, p. 14). Las asociaciones se expresan como condiciones atributo-valor y deben repetirse determinada cantidad de veces en los datos (Servente, 2002, p. 17).

El objetivo del *clustering* consiste en descubrir grupos y estructuras en los datos que son, de una u otra manera, "similares", sin utilizar datos etiquetados (Pathak et al., 2011, p. 479). Se analizan los datos y se generan conjuntos de reglas que agrupen y clasifiquen los datos futuros (Kotu y Deshpande, 2015, p. 14). De esta manera, este algoritmo permite identificar subconjuntos (*clusters)* en los datos mediante la aplicación de funciones de distancia (Servente, 2002, p. 17). Existen dos tipos de agrupamiento: jerárquico y partitivo. El primero, construye una jerarquía de *clusters* utilizando un dendograma con las distancias que existen entre los elementos del conjunto de datos, las que también pueden representarse mediante una matriz. Este algoritmo suele ser aglomerativo (*bottom-up*),

donde se dividen los *clusters* en *subclusters* que posteriormente son anidados con los que se generan en las etapas siguientes; o bien divisivo (*top- down*), donde todos los elementos son asignados a un solo *cluster* hasta que cada uno se convierte en un *cluster* individual (Pathak et al., 2011, pp. 479-480). El segundo, realiza una sola partición de los elementos en determinada cantidad de grupos, que debe especificarse con anterioridad. Tal es el caso del algoritmo k-medias: divide los datos en *k* subconjuntos, calcula los centroides (punto medio) de cada uno y asigna cada punto al centroide más cercano. Al ser un proceso iterativo, se recalcula el valor de lo los centroides hasta que converja.

Con relación a la detección de anomalías, la misma se puede definir como el problema de encontrar patrones en un conjunto de datos que no se ajusten al comportamiento deseado o normal. Se utiliza un conjunto de entrenamiento y un conjunto de detección para probar si éste contiene puntos anómalos los cuales, según Samuelsson (2016, como citó Valdés Rabelo, 2020, p. 32), pueden modificarse con el tiempo. En este sentido, las anomalías pueden ser puntuales, secuenciales y contextuales. Las primeras ocurren cuando un único punto se desvía del patrón considerado normal; las segundas, cuando una secuencia o colección de puntos es anómala con relación al resto de los datos; y las terceras, cuando un punto o secuencia de puntos son anómalos con respecto a su vecindad local (Valdés Rabelo, 2020, pp. 33 y 34).

2.4 Predicción de delitos: RL y k-NN

Los métodos de regresión son un tipo de técnica de análisis predictivo en la que la variable objetivo se relaciona funcionalmente con las variables de entrada. La RL es técnicamente un método de clasificación, cercano en su aplicación a los árboles de decisión o a los métodos bayesianos, pero estructuralmente es similar a la Regresión Lineal (Kotu y Deshpande, 2015, p. 14). La RL binaria ha sido utilizada en diversos estudios de investigación cuyo objetivo era modelar decisiones binarias o representar la ocurrencia binaria de un evento (Bell et al., 1990, p. 33).

La idea subyacente en la Regresión Lineal es la construcción de una función que explique y prediga el valor de la variable objetivo, dados los valores de las variables predictoras. Es decir, representar la variable que ha de ser predicha en términos de otras variables o

atributos, las cuales deben ser numéricas. De este modo, el problema se reduce a encontrar la línea recta que mejor explique esta tendencia (Kotu y Deshpande, 2015, pp. 167-168).
Con más de dos predictores, la variable dependiente puede expresarse como una combinación lineal de las variables independientes:

$$y = b_0 + b_1x_1 + b_2x_2 + ... + b_nx_n \quad (1)$$

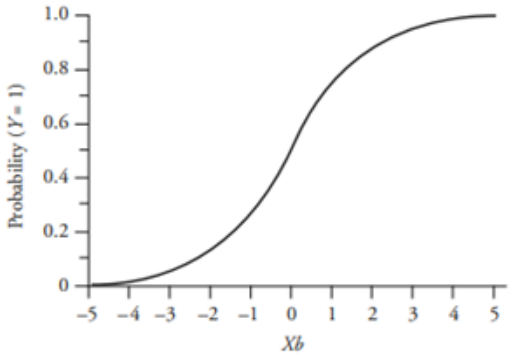
El objetivo de la RL consiste en encontrar el modelo que mejor se ajusta para describir la relación entre la variable dependiente y las variables independientes (Prabakaran y Mitra, 2018, p. 6). Es decir, resuelve el problema de predicción de una variable objetivo, la cual puede ser binomial o binaria, usando atributos numéricos.

Si la variable dependiente *y* es binomial (delito violento y delito no violento), el desafío es encontrar una ecuación que conecte funcionalmente los predictores *x* con la variable dependiente *y,* que sólo puede tomar dos valores: 0 ó 1. Sin embargo, los predictores no tienen restricciones ya que pueden ser continuos o categóricos, siendo su rango funcional también irrestricto entre $-\infty$ y $+\infty$. Para superar este problema, se debe transformar la función continua en una discreta. El concepto de *logit* es lo que permite conseguir este cometido.

A diferencia de la línea recta de la Regresión Lineal, la curva sigmoidea de la RL ajusta mejor a la mayoría de los datos. De este modo, la RL es el proceso de obtener una curva no lineal que se ajuste a los datos cuando la variable objetivo es discreta (Cramer, 2002). Como se exhibe en la Figura 1, para la ecuación $X_b = b_0 + b_1X_1$, la curva de la RL puede graficarse de la siguiente manera:

Figura 1

Curva de la RL para la probabilidad que Y = 1



Nota. Tomado de *Statistics in criminal justice* (p. 556), por D. Weisburd y C. Britt, 2014, Springer.

Ahora bien, cabe preguntarse cómo la RL encuentra la curva sigmoidea. Como se desprende de la Ecuación 1, una línea recta puede representarse con dos parámetros: la pendiente b_1 y el intercepto b_0. La forma en que las *x* y la *y* están relacionadas puede especificarse a través de b_1 y b_0. No obstante, la curva sigmoidea es más compleja y representarla paramétricamente no resulta tan sencillo, por ello, la clave radica en encontrar los parámetros matemáticos que relacionan ambas variables.

Si se transforma la variable objetivo *y* al logaritmo de las *odds* de *y*, entonces dicha variable transformada está linealmente relacionada a los predictores *x*. En la mayoría de los casos en los que se necesita usar RL, la *y* es usualmente un tipo de respuesta del estilo sí/no. Esto suele interpretarse como la probabilidad de ocurrencia de un evento (y = 1) o no (y = 0). Esto puede explicitarse de la siguiente manera:

- Si *y* es un evento (sí/no), y
- *p* es la probabilidad de que el evento ocurra (y = 1),
- entonces (1 – p) es la probabilidad de que el evento no ocurra (y = 0), y
- p/(1 – p) es el *odds* ratio, es decir, las *odds* de que el evento suceda.

El logaritmo de las *odds* de *y*, log (p/1 – p), se denomina función *logit* de *y*. Puede expresarse como una función lineal de los predictores *x*, similar a la planteada en la Ecuación 1:

$$\text{logit} = \log p/(1-p) = b_0 x + b_1 \quad (2)$$

En lugar de predecir *y*, se predice el logaritmo de las *odds* de obtener un 1 en la variable dependiente. El *odds ratio* brinda una estimación para una única unidad de incremento en la variable independiente. Como no es una función lineal de los coeficientes, no se puede afirmar que para cada unidad de incremento en la variable dependiente, el *odds ratio* aumenta en la misma proporción.

En el caso que se involucren múltiples variables independientes, la ecuación se estructura de la siguiente manera:

$$\text{logit} = b_0 + b_1 x_1 + b_2 x_2 + ... + b_n x_n \quad (3)$$

El *logit* puede tomar cualquier valor entre –∞ y +∞. Para cada fila de predictores de un *dataset*, se puede computar el *logit*. Esto es, los valores predichos de *y* obtenidos de la ecuación de regresión varían entre 0 y 1, a pesar de que los resultados de la regresión pueden alcanzar cualquier valor entre –∞ y +∞. Con el *logit*, es sencillo computar la probabilidad de ocurrencia o no de *y*. Esta ecuación se conoce con el nombre de función de probabilidad acumulada:

$$p = e^{\text{logit}}/(1 + e^{\text{logit}}) \quad (4)$$

El modelo de RL de la Ecuación 3 proporciona, en última instancia, la probabilidad de ocurrencia de *y* (y = 1) dado valores específicos de *x* mediante la Ecuación 4.

Utilizando las Ecuaciones 3 y 4, y conociendo previamente los valores de *x*, se puede calcular el valor de *p*. Para ello, se necesita determinar los coeficientes *b* de la Ecuación 3. Suponiendo un valor inicial de prueba para *b*, y dada una muestra de datos de entrenamiento, se puede calcular:

$$p^y * (1 - p)^{(1-y)} \quad (5)$$

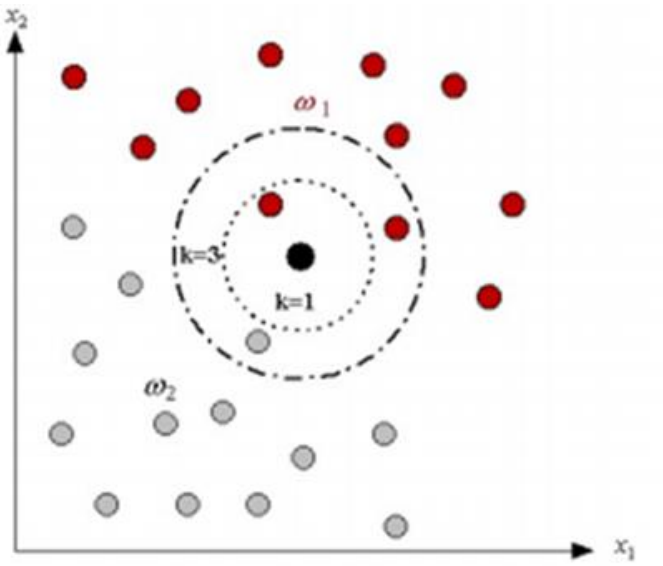
donde *y* es la variable objetivo original y *p* es la probabilidad estimada usando la Ecuación 4.

Como afirman Fix y Hodges (1951, como citó García Jiménez, 2010, p. 24), el método k-NN es una técnica de aprendizaje conocida como aprendizaje basado en instancias o ejemplos (*instance-based learning*), que se circunscribe a "memorizar" los datos de entrenamiento. La premisa subyacente a este razonamiento radica en que los miembros de una población comparten características y propiedades similares con los individuos que la rodea (García Jiménez, 2010, p. 24).

En el aprendizaje supervisado, los problemas de agrupamiento consisten en organizar un conjunto de elementos en grupos según una lógica de similitud o proximidad, para lo cual se utiliza una función o métrica de distancia (Pérez Verona y Arco García, 2016, p. 44). La cercanía entre las instancias determina la pertenencia a determinado grupo: se presume que un elemento es más similar o afín con los elementos de su grupo que con relación a los elementos de un grupo diferente. Si por ejemplo, se elige un valor k =1, una muestra cualquiera x se clasifica en la clase asociada a su instancia más cercana. Para valores $k \geq 2$, dicha muestra se asigna a la clase más representada entre las k instancias más próximas a la muestra (García Jiménez, 2010, pp. 24-25). La Figura 2 exhibe una representación gráfica del algoritmo en cuestión.

Figura 2

Clasificador basado en el algoritmo k-NN



Nota. Adaptado de *Distribución de clases no balanceadas: métricas, análisis de complejidad y algoritmos de aprendizaje* (p. 25), por V. García Jiménez, 2010, Tesis de Doctorado, Universitat Jaume I.

De este modo, y considerando la estructura de los datos del conjunto de entrenamiento, el cálculo de distancias para estimar la proximidad entre dos instancias resulta fundamental (Cover y Hart, 1967; Cong et al., 2015). La exactitud que arroja el método de clasificación depende del modo en que se calculan las distancias entre los diferentes ejemplos (Cong et al., 2015).

Como señalan Pérez Verona y Arco García (2016, p. 44), en concordancia con lo expuesto por Bellet et al. (2013, p. 10), la aplicación D: $X \times X \rightarrow \Re+$ sobre un espacio X se denomina métrica si $\forall\ x_i, x_j, x_k \in X$ se satisfacen las siguientes condiciones:

a) Desigualdad triangular: $D(x_i, x_j) + D(x_j, x_k) \geq D(x_i, x_k)$ (6)

b) No negatividad: $D(x_i, x_j) \geq 0$ (7)

c) Simetría: $D(x_i, x_j) = D(x_j, x_i)$ (8)

d) Identidad: $D(x_i, x_j) = 0 \Leftrightarrow x_i = x_j$ (9)

La función se denomina pseudométrica sólo si satisface las primeras tres propiedades. Como sostienen Deza y Deza (2009, como citó Pérez Verona y Arco García, 2016, p. 44), la medida de similitud más popular para datos numéricos por su simplicidad y

características de generalización es la distancia euclidiana, a pesar de que existen diversas métricas como la similitud coseno, la distancia de Mahalanobis, de Levenshtein, entre otras.

La distancia euclídea se calcula con la fórmula detallada a continuación y el valor escalar resulta de los valores de los atributos de las dos instancias (García Jiménez, 2010, p. 25):

$$d(\mathbf{y},\mathbf{x}) = \sqrt[2]{\sum_{j=1}^{n}(y_j - x_j)^2} \tag{10}$$

Con relación a las ventajas de los k-NN**,** se pueden enumerar las siguientes: el coste del aprendizaje es nulo, no debe hacerse ningún supuesto sobre los conceptos que se quieren aprender, se utilizan funciones de distancia sencillas como las aproximaciones para aprender conceptos más complejos y resulta bastante tolerante al ruido. Entre las desventajas, puede mencionarse que el costo computacional es alto, no existe un método para elegir el valor óptimo de *k* debido a que depende de los datos utilizados, no existe una descripción de los conceptos aprendidos y, si el número de descriptores aumenta, el rendimiento disminuye (García Cambronero y Gómez Moreno, 2006).

Como se mencionó precedentemente, los modelos explicados son aquellos que arrojan los resultados más exactos con relación a la predicción de ocurrencia de delitos violentos, como se demuestra en el capítulo 5 correspondiente al desarrollo de la metodología. La RL y el algoritmo k-NN, al emplearse como metodologías de cuantificación del riesgo para predecir los delitos violentos, constituyen herramientas flexibles capaces de adaptarse a un contexto dinámico y cambiante producto de la utilización de conjuntos de datos abiertos, y se convierten en aliadas estratégicas en la gestión de riesgos delictivos.

No obstante, todas las técnicas propias del aprendizaje automático presentan sesgos y, por consiguiente, también los datos, pues los modelos se construyen a partir de estos últimos. En este sentido, el análisis de datos es parte constituyente de la gestión de riesgos. Si bien el uso de datos y algoritmos tienen beneficios potenciales que superan a los riesgos, se debe asumir un enfoque proactivo que fomente una toma de decisiones responsable y que contemple diversas dimensiones como la seguridad, la ética y la privacidad.

Capítulo 3: La importancia de los datos y los algoritmos: usos y limitaciones

3.1 Los sesgos de los datos y los algoritmos

Según la definición de la Real Academia Española, un sesgo es un error sistemático en el que se puede incurrir cuando al hacer muestreos o ensayos se seleccionan o favorecen unas respuestas frente a otras. El riesgo inherente a la presencia de sesgos se pone de manifiesto durante todo el proceso de gestión de datos, desde su recolección hasta la elaboración de sugerencias en base a los resultados obtenidos. El análisis predictivo o la detección de tendencias y patrones sólo acentúa los sesgos preexistentes en los conjuntos de datos empleados.

Las etapas del proceso de toma de decisiones basado en aprendizaje automático son: recolección de datos, desarrollo del modelo, validación y monitoreo y revisión. Los sesgos inherentes al aprendizaje automático, a saber el sesgo estadístico y el sesgo cognitivo, deben identificarse y controlarse en cada una de las etapas. Por un lado, el sesgo estadístico se refiere al error generado por factores relacionados con la recolección, el análisis, la interpretación o la revisión de datos. Por otro lado, el sesgo cognitivo puede entenderse como el efecto psicológico que altera el procesamiento de la información y tiene múltiples determinantes: culturales, sociales y éticos, entre otros.

La tecnología de base de datos cuenta con numerosas ventajas, entre las cuales se encuentra el uso de herramientas automáticas para analizar grandes volúmenes de datos que permiten emplearlos de maneras cada vez más eficientes, dependiendo de los requerimientos de las organizaciones, empresas y estados (Clifton y Marks, 1996). Dichas herramientas permiten conectar datos recopilados en diversos momentos y lugares y para diferentes propósitos a través de algoritmos que crean relaciones impredecibles. Las características de estos datos distan ampliamente de las de los *datasets* “tradicionales”, restringidos a un contexto próximo a su punto de recolección original (Metcalf et al., 2016). No obstante, la minería de datos no es una panacea y acarrea ciertos problemas y dificultades (Hand, 1998).

Extraer aprendizaje en base a datos y análisis basados en evidencia no resulta una tarea sencilla y dista de ser infalible. Para ello, debe evaluarse tanto la validez interna como externa de la evidencia. Se dice que un estudio tiene validez interna cuando los resultados obtenidos son correctos para el contexto del estudio realizado o la muestra escogida. No obstante, estos resultados no siempre se pueden extrapolar a otros contextos (validez externa) en los cuales no sería adecuado tomar decisiones en base a conclusiones que provengan de otras circunstancias. Es decir, resulta primordial conocer el contexto relacionado a cuándo, cómo y por qué fueron creados los datos, qué variables contienen y para qué se los utiliza. Es dable mencionar que tomar decisiones basadas en datos representa un salto cualitativo a nivel de diseño e implementación de políticas públicas, toda vez que se desestiman iniciativas basadas en evidencia anecdótica, sesgos de confirmación y falacias de evidencia incompleta (Avenburg et al., 2021).

Un ejemplo de la importancia del contexto al momento de aplicar técnicas de minería de datos lo constituye la experiencia uruguaya. El Ministerio del Interior adquirió la licencia del *software PredPol*, un sistema para predecir delitos desarrollado conjuntamente por el departamento de policía de Los Ángeles y la Universidad de California, en Estados Unidos. Dicho sistema fue utilizado entre los años 2014 y 2017. Con los datos provistos por el Ministerio y la utilización de un algoritmo de "caja negra", *PredPol* elaboraba mapas prospectivos de la ciudad de Montevideo en los que se identificaban secciones de 150 metros cuadrados en las cuales existía una alta probabilidad de comisión de delitos. A partir de dichos mapas, se asignaban los recursos de patrullaje en las diversas locaciones.

El modelo, desarrollado y aplicado en un contexto diferente al de su implementación, fue discontinuado dado que las áreas donde se operó con este *software* no mostraron mejores resultados que aquellas donde se utilizaron métodos estadísticos tradicionales. Asimismo, las limitaciones en los conjuntos de datos que se utilizaron como *inputs* (ubicación geográfica, nivel socioeconómico, origen étnico, entre otras) afectaron a determinados sectores de la población, tendiendo a generar discriminación (Ortíz Freuler e Iglesias, 2018, pp. 26-30).

El proceso de toma de decisiones basado en evidencia reviste complejidad, especialmente con relación a la calidad, la disponibilidad y la actualización de los datos. Existen problemas de almacenamiento, intercambio e insuficiencia de datos; desconocimiento

sobre las ventajas y desventajas de incorporar la evidencia en el diseño de políticas y riesgos asociados al uso de datos y de algoritmos que pueden derivar en resultados sesgados y (van Ooijen et al., 2019).

A partir de la implementación de métodos de *big data*, la producción de conocimiento contrarresta los compromisos centrales de los esquemas regulatorios y de cumplimiento. Los principios de la ética de la investigación focalizados en la condición "pública" del conjunto de datos, en vez de priorizar su uso potencial, minimizan las desventajas que pueden originarse. Este ejemplo manifiesta que las condiciones epistémicas que se integraron en la regulación de la ética de la investigación ya no se cumplen (Metcalf et al., 2016).

El uso de datos y algoritmos tiene implícito una dimensión ética y de derechos humanos, toda vez que sus aplicaciones impactan en la vida de las personas y en su derecho a la privacidad y a la protección de datos. Para ello, es preciso contar con leyes y marcos normativos que regulen estas cuestiones (Ramió, 2019).

La dimensión ética debe estar presente no sólo en todas las etapas del ciclo de vida y gestión de los datos sino también en la aplicación de algoritmos y modelos (Hagendorff, 2020)[4] que profundizan los sesgos existentes en los datos y agregan nuevos, propios de las limitaciones de las tecnologías empleadas. A pesar de que también pueden existir sesgos involuntarios, otros pueden ser intencionados dado que los algoritmos ponderan a qué factores se les atribuye mayor importancia relativa al momento de tomar decisiones incorporando, de este modo, los sesgos de los individuos que los han diseñado. Adicionalmente, esto puede devenir en la presencia de sesgos sociales relacionados con el género, la raza o etnia, etc. Por ello, puede concluirse que la minería de datos no puede tener la objetividad o neutralidad que se le quiere atribuir.

Es menester enmarcar el desarrollo de la minería de datos en los principios del humanismo tecnológico, los derechos digitales y la promoción de las tecnologías democráticas. Para ello, resulta fundamental que los organismos públicos y la ciudadanía aumenten el control

[4] Este autor también aborda el uso de algoritmos de acuerdo a los modelos de "cajas negras", en los que se desconoce cómo se transforman las variables de entrada.

democrático para asegurar que los datos y algoritmos sean transparentes y auditables y, también, establezcan algún régimen de responsabilidad por los daños que puedan causar los sesgos inherentes a los modelos utilizados.

Las leyes de privacidad y protección de datos están basadas en el control individual de la información y en principios como la minimización de datos y la denominada limitación del propósito de las fuentes de información. Minimizar la recopilación de información no constituye el enfoque más efectivo para resolver los problemas de privacidad. En contraposición, se puede construir una matriz de riesgos que considere no sólo el valor de los distintos usos de los datos sino también los riesgos potenciales para la autonomía y privacidad de los individuos. Cuando los beneficios del uso prospectivo de datos superan los riesgos de privacidad, se debería asumir la legitimidad del procesamiento incluso si las personas se niegan a dar su consentimiento (Tene y Polonetsky, 2012, p. 67).

En Cranor et al. (2016), se aborda el tema de la privacidad de los datos enfatizando las preocupaciones que surgen de la recopilación, el intercambio, el análisis y el uso de datos personales en los sistemas de información. Esto incluye la divulgación no deseada de información personal, la falta de transparencia y control sobre cómo se usa la información y la discriminación que origina dicha divulgación. Ciertos problemas de privacidad están vinculados a la aplicación de algoritmos, por ejemplo, cuando el modelo elegido puede revelar información inapropiada sobre el conjunto de entrenamiento utilizado para el análisis. Asimismo, la recopilación de datos en un único lugar físico incentiva la centralización de información e incrementa el riesgo de divulgación.

Adicionalmente, la interoperabilidad de los datos genera nuevos problemas a la privacidad que no se relacionan solamente con el riesgo de divulgación o el control individual de los datos personales. En este sentido, conjuntos de datos que en sí mismos pueden resultar inocuos y están correctamente anonimizados, pueden revelar información altamente sensible cuando son analizados en conjunto con otros *datasets*. Por lo tanto, la privacidad de los datos personales no sólo depende de la salvaguarda que se aplica al *dataset* original sino también a los conjuntos de datos restantes que se utilicen (Metcalf et al., 2016).

Las organizaciones utilizan diversos métodos de desidentificación como, por ejemplo, la anonimización, la seudoanonimización, la codificación de claves y la fragmentación de

datos para resolver preocupaciones vinculadas a la privacidad. Sin embargo, en las últimas décadas los científicos de datos afirman que los datos anónimos pueden volver a identificarse y atribuirse a personas específicas.

Si la información anónima se combina con fuentes de datos adicionales, existe un riesgo de reidentificación, es decir, la información puede ser autenticada. No obstante, los riesgos de privacidad más urgentes se explicitan sólo si hay certeza en la reidentificación. En este sentido, no sólo es necesario un conjunto de principios o políticas que regulen la privacidad sino también soluciones técnicas que aseguren a los usuarios tener un control significativo sobre sus datos. Como afirma Paul Ohm en su artículo de la *Stanford Law Review*, "la ciencia de la reidentificación interrumpe el panorama de la política de privacidad al socavar la fe que hemos depositado en el anonimato." (2010, como se citó en Tene y Polonetsky, 2012, p. 65).

Resulta difícil delimitar cuáles aspectos pertenecen al ámbito de la privacidad, que requieren consentimiento del individuo en caso de divulgación, y cuáles deben ser difundidos por referirse a asuntos de interés público. Los formuladores de políticas también deben abordar el papel del consentimiento en el marco de la privacidad. A pesar de que muchas actividades de procesamiento de información se basan en el consentimiento individual, los individuos no están preparados para tomar decisiones sobre sus datos personales de manera responsable, ya sea por los sesgos cognitivos o por la complejidad del ecosistema de información (Tene y Polonetsky, 2012, p. 67).

Actualmente, no existe un mecanismo que posibilite que los individuos puedan protegerse contra los riesgos asociados con la información no autenticada (Masiello y Whitten, 2010, pp. 122-123). Asimismo, resulta necesario aplicar códigos de buenas prácticas que definan expresamente el alcance y los resultados potenciales del proceso de tratamiento de datos personales.

Otra de las consecuencias de una gestión deficiente en el relevamiento, la recolección y el uso de datos personales es la discriminación y la marginación de determinados grupos sociales. Puntualizando en el ámbito del delito, el programa informático *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS), desarrollado por la empresa privada *Northpointe Inc*., es uno de los algoritmos más utilizados en el sistema de

justicia penal de Estados Unidos y se aplica a numerosos estados como Nueva York, Wisconsin, Florida y California. El objetivo de dicho algoritmo consiste en evaluar el riesgo de reincidencia de los presidiarios a partir de los datos personales disponibles sobre los delitos cometidos y su nivel de gravedad, el nivel de educación alcanzado y el empleo, entre otras variables (Ramió, 2019, p. 131).

Según el artículo publicado en el año 2016 por la Organización No Gubernamental (ONG) estadounidense de periodismo de investigación *ProPublica*, COMPAS realizó pronósticos racistas: los acusados afroamericanos tenían mayor probabilidad de ser juzgados incorrectamente y mayor riesgo de reincidencia en comparación con los acusados blancos, a pesar de que el atributo "raza" no se incluyó explícitamente en la predicción (Larson et al., 2016). En este caso, el uso de la minería de datos no sólo no genera ningún beneficio a la ciudadanía sino que además omite los aspectos éticos correspondientes al caso[5].

Boyd y Crawford (2012) proponen la utilización de grandes volúmenes de datos sociales y culturales que posibiliten adoptar un nuevo enfoque en el campo de las humanidades y las ciencias sociales. Asimismo, Manovich (2012) sostiene que los científicos informáticos están trabajando con este tipo de datos en lo que se denomina computación social. El desafío planteado es que aquellas personas provenientes de las ciencias sociales o del campo de las humanidades puedan utilizar programas informáticos de análisis y visualización de datos, con el objeto de combinar el enfoque cualitativo con el cuantitativo.

A pesar de los riesgos mencionados, en la literatura especializada existe consenso respecto a que la utilización de datos y algoritmos generan grandes beneficios sociales, económicos y de sostenibilidad a corto plazo y largo plazo. Sin embargo, se deben considerar todas las aristas de la problemática –ética, seguridad, privacidad, entre otras- para detectar los sesgos inherentes a los datos y algoritmos y calcular los riesgos derivados de la toma de decisiones en los distintos niveles de gobierno.

Las técnicas analíticas derivadas de la minería de datos convierten a los datos en información y conocimiento, proporcionando una base más confiable para la toma de decisiones informada. En este sentido, en el ámbito de la administración pública resulta

[5] Para mayor información, ver el caso Loomis. Disponible en: https://confilegal.com/20180402-justicia-robotica-el-caso-loomis/

fundamental utilizar los datos como activos estratégicos que permitan diseñar e implementar políticas públicas sostenibles.

3.2 Gobernanza de datos y algoritmos en el sector público

Entre la infinidad de acepciones que arroja la literatura, la gobernanza de datos puede definirse como el ejercicio de la autoridad, el control y la toma de decisiones compartida sobre cómo se gestionan los datos, sea dentro de una misma organización o entre diferentes organismos que tienen un interés común por los mismos (van Ooijen et al., 2019, p. 8). También se refiere al marco que establece derechos y responsabilidades en la toma de decisiones en el uso de datos (Khatri y Brown, 2010). Como señalan Salvador y Ramió (2020), existe cierta aceptación sobre relacionar la gobernanza de datos con las siguientes consignas: los datos son activos que las organizaciones deben gestionar, las responsabilidades en la toma de decisiones deben estar establecidas y la calidad de los datos y su adecuado uso debe estar normado. Encontrar prácticas de gobernanza de datos que mantengan un equilibrio entre la creación de valor y la exposición al riesgo es la nueva organización necesaria para explotar las ventajas competitivas y maximizar el valor agregado del uso de *big data* (Tallon, 2013).

En Janssen et al. (2017, pp. 189 y 192), se abordan cuestiones relacionadas con los procesos de innovación del sector público basados en el uso de grandes volúmenes de datos y de datos abiertos. Asimismo, se enumeran algunos factores que influyen en la innovación basada en datos y se los clasifican en cuatro dimensiones: estratégica y política, organizacional, gobernanza de datos y tecnológica. Con relación a la gobernanza de datos, se destacan las siguientes características: acceso (abierto, semi-abierto o cerrado) y calidad (exactitud, veracidad e integridad) de los datos, capacidad para procesarlos, compartirlos y reutilizarlos, y normativa de acceso y privacidad.

Otra de las ventajas de la tecnología de base de datos es el intercambio de información, incluyendo aquel que se realiza con otras organizaciones (Clifton y Marks, 1996) para evitar que se trabaje en “silos”. No obstante, en el sector público existen diversos obstáculos para intercambiar datos con otras organizaciones y dentro de las mismas reparticiones del gobierno, contribuyendo a crear un ambiente de falta de transparencia y

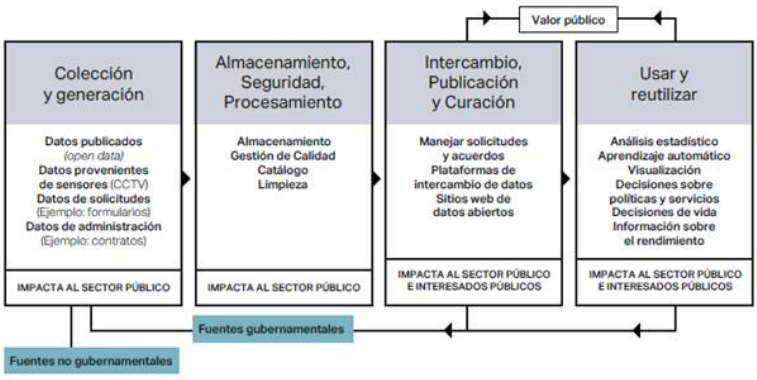
desconfianza en la información que los datos pueden aportar. El desconocimiento sobre el valor de los datos, en términos monetarios y de información, afecta la disponibilidad y la calidad de los datos.

Por su parte, la adopción de técnicas propias del aprendizaje automático por parte de los gobiernos acarrea múltiples beneficios. Entre ellos, cabe mencionar un aumento de la eficacia con relación al control del gasto y la formulación de políticas, la promoción de la participación ciudadana y la mejora en la transparencia que puede redundar en servicios públicos de mayor calidad y mayor confianza en el gobierno. Entre los desafíos, cabe destacar la seguridad, la privacidad, la portabilidad y la interoperabilidad de los datos; las barreras culturales y políticas, las limitaciones tecnológicas y la gestión eficiente de los datos (Christodoulou et al., 2018). A partir de una vasta revisión bibliográfica, González-Zapata y Heeks (2015, p. 2) sostienen que existen cuatro factores que influyen en la política de datos abiertos del gobierno: burocráticos, políticos, tecnológicos y económicos, siendo los dos primeros los más relevantes.

El ciclo de valor de los datos gubernamentales puede resultar de utilidad en el diseño de políticas, en tanto anticipa tendencias y patrones y contribuye a gestionar los recursos físicos y financieros (Figura 3).

Figura 3

Ciclo de valor de los datos gubernamentales



Nota. Adaptado de *A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance* (p. 11), por C. van Ooijen et al., 2019, OECD Working Papers on Public Governance, No. 33

Para comprender las oportunidades de un sector público que se base en datos, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) identifica tres áreas en las que se desarrollan iniciativas para apoyar el proceso de toma de decisiones en todos los niveles de gobierno, a saber: gobernanza anticipatoria, diseño y entrega de políticas que satisfagan a los ciudadanos y gestión del rendimiento de los recursos.

Con relación a la gobernanza anticipatoria, ésta permite a los gobiernos responder de manera proactiva basándose en la evidencia y el conocimiento en lugar de la experiencia y el protocolo. Pronosticar significa intentar predecir las necesidades futuras a partir de los datos y las tendencias existentes (van Ooijen et al., 2019, pp. 17-18).

Adicionalmente, las técnicas de modelado y predicción basadas en datos permiten que los gobiernos puedan anticipar los desarrollos sociales, económicos o naturales plausibles de ocurrir en el futuro, así como construir sistemas de alerta temprana, realizar análisis de sentimientos de las redes sociales y diseñar sistemas de apoyo a la toma de decisiones en tiempo real (Höchtl et al., 2016, p. 50).

En América Latina, las recomendaciones pueden resumirse en tres ejes: desarrollar infraestructura y experticia gubernamental para el aprovechamiento de las técnicas propias del aprendizaje automático; asegurar la transparencia, la participación ciudadana y la rendición de cuentas en el desarrollo e implementación de dichas técnicas, y establecer un mecanismo de evaluación de riesgo previo a la implementación de sistemas automatizados (Ortíz Freuler e Iglesias, 2018, pp. 32-34).

Con relación al primer eje, resulta necesario desarrollar un ecosistema que se focalice en los siguientes actores: para asegurar la efectividad, técnicos que desarrollen y dominen los sistemas necesarios para procesar la información; para asegurar la legitimidad, organismos reguladores y de control; para asegurar la transparencia, la participación de la ciudadanía; para identificar los grupos afectados, las organizaciones de la sociedad civil; y para fomentar el desarrollo económico y de los recursos humanos, las pequeñas y medianas empresas (Ortíz Freuler e Iglesias, 2018, p. 32).

El segundo eje tiene por objeto garantizar la legitimidad del proceso de modernización del estado así como la calidad de los resultados derivados de la aplicación de las técnicas

propias del aprendizaje automático para evitar robustecer sesgos o inequidades preexistentes, ofreciendo un marco teórico que enaltezca los derechos humanos y los principios democráticos (Ortíz Freuler e Iglesias, 2018, p. 33).

Con relación al último eje, es dable mencionar que en la región está creciendo paulatinamente el interés por el uso de estas herramientas en el marco de las políticas públicas. Ante los riesgos de su utilización, es menester establecer criterios que permitan a las administraciones gubernamentales discriminar aquellos algoritmos que puedan ser problemáticos (Ortíz Freuler e Iglesias, 2018, p. 34).

Asimismo, la selección de datos y la utilización de algoritmos deberían definirse con equipos interdisciplinarios capaces de detectar los sesgos intrínsecos o de contexto de los datos, contemplando las implicancias éticas, sociales, políticas y económicas (Ramió, 2019). Queda expuesto que resulta fundamental para los gobiernos recopilar, combinar y compartir datos de diversas fuentes con el objeto de modelar políticas públicas y respaldar sus decisiones de gestión.

3.3 La transparencia de los gobiernos en la era del *big data*

A partir de la aparición de las Tecnologías de la Información y la Comunicación (TIC) y, por supuesto, de internet, los gobiernos han podido almacenar y difundir más fácilmente la información, promoviendo lo que suele denominarse transparencia mediada por computadoras. En este sentido, la transparencia es propuesta como una solución a una de las problemáticas más intangibles de la gobernabilidad democrática: la creciente desconfianza de los ciudadanos hacia los gobiernos (Grimmelikhuijsen et al., 2013, p. 575).

En términos generales, la transparencia se vincula con las medidas implementadas por cualquier organización para disponibilizar información relevante sobre sus procesos de procedimiento, funcionamiento, desempeño y toma de decisiones. Esto implica, entre otras cosas, que cualquier individuo fuera de la entidad puede monitorear las actividades y decisiones tomadas dentro de la misma. Con relación a la transparencia, y siguiendo los

lineamientos del artículo de Grimmelikhuijsen et al. (2013, p. 576), se describen tres propiedades de la información, a saber: la exhaustividad, el color y la facilidad de uso.

En primera instancia, la exhaustividad hace referencia a si la información se divulga en su totalidad. Para Moon y Norris (2005, como se citó en Grimmelikhuijsen et al. 2013, p. 576), la transparencia se vincula con la cantidad de información disponible en las páginas web oficiales de los gobiernos. No obstante, esta propiedad no debe confundirse con la cantidad de información disponible: las administraciones gubernamentales que publican demasiada información mediante informes de políticas inexactos pueden considerarse menos transparentes que aquellas que divulgan contenido escueto pero preciso.

Por su parte, el color de la información refiere a su nivel de positivismo. Como sostienen Davis, Etzioni y Porumbescu (1999, 2010 y 2013 respectivamente, como se citó en Grimmelikhuijsen et al., 2013, p. 576), una gran cantidad de académicos coinciden en que la información publicada en las páginas web de los gobiernos tiende a ser demasiado positiva sobre sus iniciativas y/o funcionarios. Por lo tanto, el grado en que la información está teñida por una interpretación políticamente favorable de la "verdad" adquiere una relevancia capital para este análisis.

La tercera dimensión central de la información en un sitio web se vincula con su usabilidad: no sólo es importante su divulgación sino también la manera en que se disponibiliza al público. En este sentido, Dawes y Larsson (2010 y 1998 respectivamente, como se citó en Grimmelikhuijsen et al., 2013, p. 576) afirman que la transparencia implica que la información se divulgue en un formato comprensible y de manera oportuna.

A modo de conclusión, el estudio indica que la transparencia no siempre tiene un efecto positivo en la confianza pública en el gobierno y, además, varía notablemente entre un país y otro dependiendo del contexto cultural. De hecho, la transparencia en el funcionamiento del análisis de datos podría facilitar su manipulación, influyendo en el resultado de dicha analítica. Incluso si un gobierno está dispuesto a someter los procesos de formulación de políticas al escrutinio público, el enfoque basado en datos puede generar más opacidad y socavar la transparencia gubernamental (Lammerant y Hert, 2016).

En esta línea, Kuehn y Salter (2020, p. 2590) seleccionan en su investigación cuatro desafíos globales que los gobiernos deben enfrentar en la era digital: las noticias falsas (*fake news*), los filtros burbuja[6] (*filter bubbles*) y las cámaras de eco[7] (*echo chambers*), el discurso de odio (*hate speech*) y la vigilancia digital (*digital surveillance*). Para estos autores, dichos desafíos constituyen amenazas digitales a los procesos democráticos. No obstante, aún no existe consenso sobre cómo funcionan o cómo combatirlas. Con la circulación de tanta información, el conocimiento empírico se ve empañado por el gran volumen de datos, los silos interdisciplinarios y los intereses particulares de las agendas políticas de los gobiernos.

Las *fake news* comprenden algunas prácticas antidemocráticas. Según la bibliografía relevada por estos autores, pueden definirse como el contenido informativo caracterizado por la desinformación o información deliberadamente engañosa, los objetivos políticos diseñados para moldear la opinión pública sobre diversos temas o personas, la reactividad o capacidad de evocar una fuerte respuesta emocional, la capacidad de propagación o difusión rápida dentro y entre las redes y los mensajes personalizados extraídos de los datos de comportamiento de los usuarios. Estas últimas dos características se vinculan a los objetivos de lo que Zuboff (2019, como se citó en Kuehn y Salter, 2020, p. 2592) denomina capitalismo de vigilancia: explotar datos personales para predecir, modificar y lucrar con el comportamiento de los individuos.

Los ecosistemas personalizados en línea pueden reducir el alcance de información, las opiniones y los recursos que los usuarios encuentran. Los filtros burbuja tienen efectos adversos sobre el discurso cívico y la democracia al facilitar el aislamiento informativo, sea intelectual e ideológico, y proporcionar información que sólo es consistente con la manera de pensar del usuario. Lo mismo sucede con las cámaras de eco: son el producto de las interacciones entre los filtros burbuja y la tendencia a buscar información que se corresponde con el conocimiento previo sobre el tema en cuestión. Como afirman Ceron y Memoli (2016, como se citó en Kuehn y Salter, 2020, p. 2593) este sesgo de confirmación,

[6] Un filtro burbuja es el resultado de una búsqueda personalizada en la que el algoritmo de una página web selecciona, a través de predicciones, la información que al usuario le gustaría ver, basándose en información sobre él mismo.

[7] La cámara de eco es un concepto metafórico ligado a los medios de comunicación de masas y se basa principalmente en que un conjunto de ideas del mismo segmento informativo o ideológico se amplifica y se transmite en un sistema hermético, donde lo diferente se censura o se prohíbe.

sumado a los efectos de la polarización, son reforzados por el contenido político que explota esta debilidad.

Asimismo, las redes sociales amplifican las expresiones de odio hacia sectores marginados o vulnerables, lo que potencialmente provoca efectos psicológicos en los destinatarios de estos mensajes e incrementa las desigualdades existentes. Estos discursos pueden estar motivados por cuestiones raciales, étnicas o religiosas: su auge es consecuencia de factores geopolíticos, ideológicos y socioculturales más que del capitalismo de vigilancia (Kuehn y Salter, 2020, p. 2593).

Por último, la vigilancia digital hace referencia a la recopilación y análisis sistemáticos de datos digitales por parte de actores organizacionales con el propósito de regular el comportamiento. Algunos estudios realizados a periodistas y escritores indican una correlación positiva entre la percepción de la vigilancia gubernamental y la autocensura. La vigilancia digital excede el marketing conductual cuando se utiliza por los gobiernos con fines políticos, de gestión o de control de la población. Como afirma Gorwa (2019, como se citó en Kuehn y Salter, 2020, p. 2595), la falta de transparencia relacionada con la gestión de datos pone de manifiesto otros problemas vinculados a la libertad de expresión, la participación política y la gobernabilidad democrática.

En este marco, surge el planteamiento de soluciones tecnológicas, regulatorias y culturales para contrarrestar las amenazas digitales. Como señalan algunas investigaciones, el diseño y las prestaciones de una plataforma digital pueden contribuir a reducir la mayoría de las amenazas actuales. También existen propuestas de creación de algoritmos que identifiquen contenidos de búsqueda “creíbles” o filtros que permitan a los usuarios elegir el tipo de contenido que encuentran. La regulación constituye otra de las herramientas utilizadas para combatir estas amenazas, especialmente la relacionada con la vigilancia digital. Los gobiernos pueden prevenir infracciones y desincentivar los abusos en la gestión de datos y de información. Las llamadas “soluciones culturalmente integradas en una dimensión cívica” están diseñadas para que los usuarios tengan mayor poder de elección y decisión sobre sus experiencias en línea, como por ejemplo fomentar la capacitación en pensamiento crítico, la alfabetización mediática y la educación en torno a la función y el poder de los algoritmos (Kuehn y Salter, 2020, pp. 2595-2600).

A modo de conclusión, existen escasos estudios que aborden estas amenazas como fenómenos derivados de las condiciones digitales estructurales que generan desconfianza en las instituciones democráticas. Los investigadores enmarcan esta temática como problemas individuales y aislados que pueden solucionarse con tecnología y regulación. En el marco de los derechos y garantías jurídicas de la ciudadanía, la problemática de los datos y los algoritmos radica no sólo en los sesgos sino también en la falta de transparencia.

Capítulo 4: Predicción de delitos en el ámbito internacional y nacional

4.1 Predicción de delitos en el ámbito internacional

En las últimas décadas, se han realizado una gran cantidad de investigaciones científicas sobre la minería de datos aplicada al análisis y predicción del delito (Reza et al., 2011, p. 873; Chen et al., 2004), principalmente debido a la enorme cantidad de información que requiere la utilización de herramientas computacionales potentes que permitan identificar patrones y tendencias en las variables involucradas.

La interpretación manual de los datos relacionados con delitos está limitada al tamaño de los conjuntos de datos y a la complejidad que existe entre los diferentes atributos criminales. En este sentido, las técnicas de minería de datos aceleran y mejoran la calidad de los análisis criminales y generan soluciones en tiempo real para ahorrar no sólo recursos sino también tiempo (Shojaee, 2013, p. 361).

A continuación, se describen algunas experiencias internacionales relevantes en materia de aplicación de minería de datos en el análisis de información criminal.

En el año 1997, se lleva a cabo el proyecto COPLINK a partir de la colaboración entre los investigadores del Laboratorio de Inteligencia Artificial de la Universidad de Arizona y los departamentos de policía de Tucson y Phoenix, en Estados Unidos (Chen, Atabakhsh et al., 2003; Chen et al., 2004). El mismo contiene dos grandes componentes: COPLINK CONNECT, que busca compartir información de distintas fuentes entre los departamentos policiales, mediante un fácil acceso y una interfase sencilla, y COPLINK DETECT, que detecta de forma automática distintos tipos de asociaciones entre las bases de datos mediante técnicas de minería de datos (Reza et al., 2011, p. 873).

Los estudios de caso pertenecientes a este proyecto incluyen la extracción automática de entidades, la detección automática de multiplicación de identidades, el análisis de autoría en los delitos informáticos y el análisis de redes criminales.

La extracción automática de entidades a partir de los reportes policiales permite disponer de determinada información criminal como nombres propios, características personales, datos de vehículos y domicilios (Chen, Chung et al., 2003). Para ello, como sostienen Chau et al. (2002, como se citó en Perversi, 2007, p. 12), se utiliza un algoritmo que realiza las siguientes tareas: identifica sustantivos de documentos basándose en análisis sintáctico, compara cada palabra de la oración con una base de entidades que generan valores binarios para indicar coincidencia y utiliza una red neuronal para predecir el tipo de entidad más factible.

La detección automática de multiplicación de identidades permite, a través de una base de datos de sospechosos, detectar situaciones en las que un mismo individuo tiene distinta identidad, sea de manera intencional o por un error en la carga de datos. Según los expertos, la identidad de un individuo se puede reducir a cuatro atributos: nombre, fecha de nacimiento, domicilio y número de seguridad social. La técnica implementada elige pares de registros y calcula la proximidad entre las cadenas de caracteres de cada uno de los atributos a partir de la distancia euclidiana (Wang et al., 2002, como se citó en Perversi, 2007, p. 12).

El análisis de autoría en los delitos informáticos permite rastrear automáticamente las identidades de los criminales a partir de mensajes que publican en internet. Con algoritmos de aprendizaje inductivos como los árboles de decisión, las redes neuronales de retropropagación y las SVM se buscan marcadores de estilo, características estructurales y específicas en el contenido de dichos mensajes para construir modelos que permitan identificar a los autores (Chen, Chung et al., 2003).

Para el análisis de redes criminales, se utilizan los reportes de incidentes criminales como fuentes de información y con la técnica *concept space* se identifican posibles redes de sospechosos (los criminales que cometen delitos juntos suelen estar relacionados). Luego, se detectan subgrupos dentro de una red basados en la fuerza del vínculo entre dos sospechosos utilizando *clustering* jerárquico y se aplica *blockmodeling* para revelar los patrones de interacción entre dichos subgrupos. Por último, y para uno de ellos, se calculan distintas medidas que permiten determinar el miembro clave de la red criminal (Chen, Chung et al., 2003).

Como afirma Perversi (2007, p. 12), el proyecto OVER se crea en el año 2000 en Reino Unido a partir de la colaboración conjunta del departamento de policía de West Midlands y el Centro de Sistemas de Adaptación y División de Psicología de la Universidad de Sunderland. Según Zeleznikow (2005, como se citó en Perversi, 2007, p. 13), los objetivos primarios de dicho proyecto consisten en identificar no sólo los recursos para implementar estrategias eficientes de detección y prevención sino también la información relevante que pudiera recogerse de la escena del delito. Asimismo, tiene como finalidad generar evidencia empírica que permita diseñar planes policiales interdepartamentales para reducir el delito, obtener datos que permitan nutrir el sistema de información criminal y analizar la geolocalización de los hechos para validar conjeturas sobre patrones y tendencias.

A partir de los registros de robo a viviendas particulares, las predicciones se realizan utilizando redes bayesianas y redes neuronales de Kohonen que posibilitan la confección de los perfiles de los delincuentes de acuerdo a su modo de proceder y a su vinculación con los delitos no resueltos.

Es dable destacar que existen otras experiencias internacionales de aplicación de técnicas de minería de datos para predecir delitos o patrones delictivos que, aunque menos difundidas, merecen ser mencionadas (Perversi, 2007, p. 13).

En el año 2005, la policía estatal de Illinois, en Estados Unidos, adquiere un *software* de minería de datos de la compañía *RiverGlass Inc*. con el objetivo de analizar la información criminal en tiempo real. Dicha información incluye datos de seguridad marina en los puertos hasta casos de fraude financiero. Por su parte, el Departamento de Policía de Nueva York inicia ese mismo año el proyecto *Real Time Crime Center* cuyo objeto consiste en conformar un *data warehouse* y cruzar datos de todo tipo a través de técnicas de inteligencia de negocios para detectar patrones de comportamiento e identificar asociaciones previamente desapercibidas (Valenga et al., 2007, p. 261).

En el año 2007, el departamento de policía de Ámsterdam en Holanda aplica árboles de decisión y redes neuronales de retropropagación para analizar registros criminales, con la utilización de un *software* denominado *DataDetective*. Esta iniciativa permite reconocer las causas del comportamiento criminal (por ejemplo, los casos de reincidencia) y de los delitos en ciertos barrios. Utilizando algoritmos *fuzzy*, se procede a identificar no sólo los

delitos similares relacionando casos resueltos con no resueltos sino también las zonas de aumento del delito (por ejemplo, para la localización de equipos preventivos en operativos de búsqueda de armas). Asimismo, la utilización de este *software* contribuye a la evaluación del desempeño policial (Perversi, 2007, p. 13).

En el año 2007 en Virginia, Estados Unidos, el departamento de policía de Richmond desarrolla una aplicación para el análisis de información criminal mediante el *software Clementine* que combina técnicas de minería de datos. El principal objetivo consiste en optimizar la asignación de recursos de manera proactiva y no reactiva: el resultado es una reducción del 49% en los casos de heridos con armas de fuego con un menor requerimiento de personal policial. En el mismo año, el departamento de policía de San Francisco desarrolla junto a IBM la aplicación *CrimeMaps*, *software* que permite a los policías, mediante un simple explorador web, buscar un determinado tipo de crimen, realizar análisis de *clustering* y fijar niveles umbrales de alerta temprana para un determinado delito y zona considerando los valores históricos (Valenga et al., 2007, p. 261).

Chen et al. (2008) utilizan un modelo estacionario autorregresivo y de medias móviles (ARIMA) para predecir delitos contra la propiedad en una ciudad de China y lo comparan con los modelos SES (*simple exponential smoothing*) y HES (*holt two-parameter exponential smoothing*) para determinar cuál arroja una exactitud mayor en la predicción. Siendo el modelo ARIMA el que mejor se ajusta a los datos, este estudio contribuye a que los departamentos policiales y los gobiernos municipales tomen decisiones eficientes relacionadas a la prevención de este tipo de delitos.

En el año 2016, el Instituto Nacional de Justicia de Estados Unidos lanza un desafío denominado *Real-Time Crime Forecasting Challenge* para que los científicos de datos propongan algoritmos que permitan pronosticar dónde ocurrirán los hechos delictivos en la ciudad de Portland. Para el período comprendido entre el 1 de marzo de 2012 y el 28 de febrero de 2017, el Instituto publicó los registros de llamadas de emergencia (*calls-for-service)* con sus correspondientes ubicaciones. Dichos registros contienen cuatro categorías de delitos, a saber: robo (residencial y comercial), delito callejero, robo de vehículos y una que incluye todas las tipificaciones anteriores. Las previsiones pueden realizarse para todas o algunas de las categorías utilizando un horizonte temporal de una y dos semanas; uno, dos y tres meses. Asimismo, el Instituto brinda un archivo complementario que contiene un

mapa de Portland constituido por polígonos, donde cada uno representa una pequeña sección de la ciudad (Instituto Nacional de Justicia [INJ], s.f.).

Para evaluar la capacidad predictiva de los modelos propuestos, los criterios de evaluación seleccionados por el Instituto son el Índice de Precisión de Predicción (*Prediction Accuracy Index*, PAI) y el Índice de Eficiencia de Predicción (*Prediction Efficiency Index***,** PEI). A continuación, y a fines de destacar algunos modelos alternativos en la predicción de zonas calientes (*hotspots*) de delitos, se exponen tres de los trabajos mejores rankeados ganadores del desafío (INJ, s.f.).

En Lee et al. (2017), se calcula para cada mes la probabilidad de cometer un delito utilizando la distribución *Poisson* basándose en las distribuciones de delitos de los últimos doce meses. El pronóstico se realiza para las cuatro categorías de delitos con la siguiente regla de decisión: si la probabilidad *Poisson* supera el 0,5 y el hecho delictivo ocurrió en el mes pronosticado, a la celda de la cuadrícula le corresponde un 1 (en caso contrario, el valor es cero). Sólo en el caso de los robos se considera una probabilidad igual a cero.

Para pronosticar las ubicaciones de las zonas calientes, se calculan las probabilidades de *Poisson* utilizando Microsoft Excel. Posteriormente, se evalúa el estado del riesgo en una celda de cuadrícula. La categoría que incluye a todos los delitos arroja la mejor previsión, alcanzando entre un 72% y 74% de exactitud. Asimismo, las ubicaciones de los delitos callejeros también alcanzan un alto nivel de precisión.

Por su parte, Koontz (2017), mediante la utilización de MATLAB, emplea un método de suavizado *kernel* para estimar la función de densidad de probabilidad de las ubicaciones correspondientes a las llamadas de emergencia, las cuales son muestras de una distribución bivariada. Para ello, utiliza los datos de robo (residencial y comercial) y robo de vehículos para el año calendario 2016 como conjunto de entrenamiento, los datos de enero de 2017 de estas dos categorías como conjunto de prueba; y los datos del mapa de la ciudad provisto por el Instituto. Una de las combinaciones propuesta por Koontz (ganadora del desafío) es la categoría robo con un período de tiempo de una semana y un criterio de evaluación PEI.

Para maximizar directamente el PAI en las previsiones delictivas, Mohler y Porter (2017) plantean la utilización de un método que, conjuntamente, selecciona el tamaño y la orientación de la cuadrícula óptima y aprende una función de puntaje. Para ello, utilizan las cuatro categorías de delitos y todos los períodos de tiempo disponibles. Entre los modelos seleccionados, el RF arrojó mejores resultados para aquellas previsiones con un período de tiempo de dos y tres meses, mientras que la Regresión Logística "dispersa" lo hizo para períodos de menor duración. Resulta dable destacar que cada modelo utiliza configuraciones de cuadrícula diferentes a pesar de la similitud en los puntajes de los PAI. Asimismo, los valores relativos de PAI se incrementan considerablemente cuando se utiliza una cuadrícula rotacional en vez de una fija.

Rummens et al. (2017) plantean la aplicación del análisis predictivo del delito a una ciudad de más de 250.000 habitantes en Bélgica. Para ello, se analizan retrospectivamente tres tipos de delito, a saber: robo en la propiedad, robo en la vía pública y agresión, en cuadrículas de 200 metros por 250 metros. Basándose en los datos de los tres años anteriores, se aplica un modelo ensamblado para resumir los resultados de la RL y las redes neuronales con el objeto de obtener predicciones quincenales y mensuales para el año 2014. La evaluación del modelo se realiza a través de la tasa de aciertos (*hit rate*), la precisión y el índice de predicción. Los resultados de las predicciones quincenales indican que, aplicando análisis predictivo a los datos, se pueden obtener predicciones más adecuadas. Se concluye que los resultados pueden mejorarse considerablemente comparando las predicciones quincenales con las mensuales y dividiendo los delitos cometidos durante el día y la noche.

En Vancouver, Canadá, a partir de los datos sobre delitos correspondientes al periodo 2003-2008, se aplican los k-NN y los árboles de regresión. Se realizan tareas de recolección y clasificación de datos, identificación de patrones, predicción y visualización de un *dataset* con 560.000 registros. A pesar de que la exactitud arrojada por los modelos es baja (entre 39% y 44%), el estudio concluye que esta métrica puede mejorarse ajustando ambos métodos y el conjunto de datos para alcanzar objetivos específicos (Kim et al., 2018).

En Tabedzki et al. (2018), se emplea el aprendizaje automático para predecir las estadísticas relacionadas con el delito en la ciudad de Filadelfia en Estados Unidos. Para

ello, se utiliza un conjunto de datos con las características consideradas relevantes incluyendo, además, datos sobre el clima y valores de las viviendas, y se lo divide en tres subconjuntos. Posteriormente, se plantea la problemática alrededor de tres ejes: determinar si el delito ocurre, la ocurrencia propiamente dicha y el delito con ocurrencia más probable. Se aplican métodos basados en árboles, RL y regresión ordinal y los k-NN, logrando alcanzar un 66% de exactitud para predecir la ocurrencia y un 47% para el número de delitos.

En Bharati y Sarvanaguru (2018), se analiza un *dataset* publicado en la página web kaggle.com que es actualizado por el departamento de policía de Chicago en Estados Unidos. El mismo contiene información sobre distintos tipos de delito, fecha, hora y coordenadas espaciales. Se aplican diferentes modelos como los k-NN, la RL, los árboles de decisión, el RF, las SVM y las redes bayesianas, siendo el primero el que arroja mayor exactitud, con un 78,7%. Con este resultado, se concluye que las técnicas de aprendizaje automático permiten predecir, detectar y resolver delitos con mayor celeridad que aquellas relacionadas con la estadística inferencial.

El objetivo del estudio de Bandekar y Vijayalakshmi (2020) en India[8] consiste en el análisis y diseño de algoritmos para reducir las tasas de delitos. La hipótesis plantea que la predicción de la ocurrencia de un delito se basa en la ubicación de la ocurrencia de delitos anteriores. Entre las técnicas empleadas, como el *clustering*, las redes neuronales bayesianas y el algoritmo *Levenberg Marquardt*, la más precisa es el algoritmo escalado (*scaled algorithm*) que, junto con el análisis de varianza (ANOVA), permiten reducir las mencionadas tasas en un 78% lo que implica una exactitud del mismo valor.

Hossain et al. (2020) analizan un conjunto de datos sobre los delitos cometidos durante el periodo 2003-2015 en la ciudad de San Francisco[9], Estados Unidos. Se utilizan árboles de decisión y los k-NN pero, para aumentar la exactitud de la predicción, se incorporan otras técnicas como el RF y el *AdaBoost* y se divide el *dataset* en delitos con ocurrencia más y menos frecuente. El mejor modelo lo constituye el RF que, junto con la aplicación de

[8] Tyagi y Sharma (2018) realizaron otro estudio sobre la predicción del delito en India.
[9] Existen estudios previos sobre esta ciudad donde la predicción de la ocurrencia de diferentes tipos de delitos se realizó a partir del supuesto de que los mismos han ocurrido con anterioridad (Chandrasekar et al., 2015).

métodos de submuestreo (*undersampling*) y sobremuestreo (*oversampling*), incrementa la exactitud al 99,16%.

En Meiliana et al. (2020), se aplica un modelo de Regresión Lineal en *Rapidminer Studio* utilizando la base de datos del departamento de policía de Los Ángeles, Estados Unidos, con 2.036.897 registros correspondientes al periodo 2010-2019. Dicha base contiene información sobre el tipo de delito, el área de ocurrencia, el horario, la edad y el sexo de la víctima así como las armas utilizadas por los delincuentes. Los resultados obtenidos indican que este modelo es lo suficientemente bueno para predecir el crimen, a partir de la obtención de un coeficiente de determinación de 0,19.

Una experiencia no asociada a ningún territorio en particular pero destacable por el análisis sistemático de literatura que incluye, se encuentra en Kounadi et al. (2020). El texto aporta una descripción del estado del arte en el pronóstico o previsión espacial de delitos (*spatial crime forecasting*). Esta manera de abordar el fenómeno resulta más abarcativa que la mera vigilancia policial predictiva (*predictive policing*) pero más limitada que la extracción de datos sobre delitos (*crime data mining*). La tarea predictiva principal es la clasificación binaria y el tipo de previsión predominante es la identificación de zonas críticas. Para esto se emplean diversos métodos basados en las estimaciones de densidad *kernel*, métodos propios del *machine learning*, enfoques de aprendizaje profundo (*deep learning*) y, también, técnicas basadas en procesos puntuales; aunque estos dos últimos métodos se emplean con menor frecuencia (Kounadi et al., 2020, pp. 16 y 19).

Dentro del enfoque de aprendizaje profundo, el algoritmo que arroja los resultados más adecuados es el Perceptrón Multicapa (*Multilayer Perceptron*, MLP) (Kounadi et al., 2020, pp. 12-13). Dentro de las técnicas propias del *machine learning*, el algoritmo RF constituye el modelo propuesto más utilizado; no obstante su poder explicativo es limitado, ya que interpretar los resultados resulta complejo. En otros términos, si bien su capacidad predictiva suele ser adecuada, funciona como una "caja negra" (*black box*) (Zhang y Wang, 2009; Breiman, 2010; Cánovas-García et al., 2017).

Volviendo a las experiencias territoriales, y ya en ámbito latinoamericano, en la Región Metropolitana de Chile se mide la incidencia de factores temporales y espaciales (fecha,

día y lugar de ocurrencia) y otros elementos de contexto en la probabilidad de ocurrencia de delitos utilizando un modelo logístico. Los resultados obtenidos corroboran ciertas hipótesis con relación al origen del delito y se emplea la información histórica disponible para implementar herramientas que colaboren en la caracterización de la probabilidad de ocurrencia de un hecho delictivo (Urzúa y Letelier Saavedra, 2018).

En las tres principales ciudades de Colombia (Ordóñez et al., 2020), se aplica un modelo basado en Máquinas de Soporte Vectorial para Regresión (*Support Vector Regression*, SRV) ajustado para la predicción de la tendencia de hurtos. Para ello, se utiliza una base de datos del sistema de información de la Fiscalía Nacional de Colombia con datos de registros del periodo 1960-2019. Los resultados, comparados con aquellos obtenidos de la aplicación de un modelo de Regresión Lineal estándar y un modelo de SRV sin ajuste, resultan herramientas valiosas para que las autoridades competentes tomen decisiones informadas en la lucha contra el hurto.

4.2 El caso argentino

Históricamente, el análisis de la información delictiva en Argentina se ha realizado a través de herramientas de estadística descriptiva que no reflejaban acabadamente la relación entre las diferentes variables ni tampoco permitían elaborar un diagnóstico dinámico de la problemática en cuestión.

Tal es el caso de la policía de la provincia de Buenos Aires que, en el periodo comprendido entre 1999 y 2002, comienza con "el diseño y diagramación de una solución centralizada de análisis y mapeo delictivo" (Pezzuchi, 2012, p. 36) con el objetivo de reformar el sistema de inteligencia policial. No obstante, recién en el año 2002 el entonces Ministro de Justicia y Seguridad aprueba la Resolución N° 1061 la cual establece la puesta en funcionamiento de un sistema de recolección, procesamiento y análisis de la información delictiva en el ámbito de las Jefaturas Departamentales de la Policía de Seguridad.

A partir de la información sobre delitos, dicha normativa establece que se debe confeccionar regularmente no sólo un mapa del delito sino que también se deben realizar informes estadísticos que permitan abordar el fenómeno de la delincuencia. Entre las

acciones implementadas para llevar a cabo este cometido, la Resolución N° 1062 del mismo año aprueba la realización de un curso de mapeo y análisis criminal cuya currícula aborda técnicas de análisis estadísticos, predicciones y otras herramientas de índole manual.

Hasta el año 2004, y como señala el entonces Ministro de Seguridad León Arslanián (2007, como se citó en Estévez, 2014, p. 79), no existe una base de datos unificada sobre delitos ni se cuenta con las herramientas informáticas que permiten analizar la información delictiva. Sin embargo, cabe mencionar tres experiencias que abordan la utilización de modelos predictivos en materia de análisis criminal.

En el año 2004, la entonces Secretaría de Seguridad Interior dependiente del Ministerio de Justicia, Seguridad y Derechos Humanos crea el proyecto Sistema Unificado de Registros Criminales (SURC) para interconectar y articular las dependencias policiales y judiciales a través de una red a la cual se pudiera acceder a un banco de datos común en tiempo real del cual, además, se pudieran realizar consultas online **(**Perversi, 2007, pp. 15-16).

En ese año, se recolectan datos de las 53 comisarías de la CABA y se registra información sobre las siguientes figuras delictivas: homicidios, violación, secuestro extorsivo de personas, robo a mano armada en general, robo a mano armada de automotores, hurto de automotores, robo en ausencia de moradores, robo en general, hurto en general y piratería del asfalto. El alcance del proyecto contempla incluir paulatinamente a las provincias.

Entre los objetivos generales del programa, cabe destacar: facilitar el proceso de toma de denuncias en sede policial, sistematizar las relaciones entre los hechos y los imputados con los denunciantes o víctimas y permitir la aplicación y uso de un banco de datos y mapas del delito basados en Sistemas de Información Geográfica (SIG) como herramientas dinámicas para automatizar tareas de administración y recopilación de datos. Dicha base de datos reúne información de diversa índole: registro de hechos, de denunciantes, de autores identificados y no identificados, de elementos robados, de autos robados, de armas secuestradas y de evidencias.

Entre las ventajas de la implementación del proyecto, cabe mencionar la sistematización desde el inicio del proceso con la denuncia policial, el seguimiento de los trámites de las

fiscalías, la normalización de los datos relacionados con el delito de todo el país y la interoperabilidad con los sistemas de información estadística como el Sistema Nacional de Información Criminal (SNIC) y la confección del mapa del delito con el consiguiente análisis geográfico de los hechos para optimizar la asignación de recursos. No obstante, en julio del 2004 con la salida de Gustavo Béliz de la cartera de Justicia, Seguridad y Derechos Humanos, el proyecto queda relegado hasta el día de la fecha.

En el año 2005, se realiza un proyecto de minería de datos con los homicidios dolosos cometidos en ese año mediante una herramienta de distribución libre denominada *Waikato Environment for Knowledge Analysis* (*Weka*). Se analizan 1810 registros provenientes del Sistema de Alerta Temprana (SAT) creado por la entonces Dirección Nacional de Política Criminal del Ministerio de Justicia y Derechos Humanos. Se aplica el algoritmo k-medias a través del cual se logra identificar tres patrones diferentes de homicidios dolosos. Se obtienen tres *clusters:* el *cluster* 0 (22%), que aglomera homicidios mayoritariamente en ocasión de robo y con arma de fuego; el *cluster* 1 (43%), caracterizado por homicidios en la vía pública con arma de fuego y sin la existencia de otro delito; y el *cluster* 2 (35%), compuesto por homicidios sin arma de fuego y en domicilio particular. Para explicar el comportamiento de los *clusters* de manera descriptiva, se utiliza un algoritmo de inducción como el árbol de clasificación. Este estudio demuestra que la aplicación de minería de datos genera valor agregado al análisis de la información y aporta nuevos conocimientos sobre el tema de estudio (Valenga et al., 2007).

Por último, en el año 2002, el Ministerio Público Fiscal de la Nación (MPFN) y el Centro de Información Metropolitana (CIM) de la Facultad de Arquitectura, Diseño y Urbanismo de la Universidad de Buenos Aires, suscriben un convenio de asistencia, complementación y cooperación con el objetivo de que el CIM confeccione un mapa del delito de la CABA con la información brindada por el MPFN.

El mencionado CIM desarrolla un Sistema de Información Territorial del Área Metropolitana de Buenos Aires (SAT/AMBA) que cuenta con una base cartográfica digitalizada del AMBA para ser utilizada por el programa *Geographical Information Systems* (GISs). Por su parte, el MPFN confecciona una base digitalizada de los delitos de autoría desconocida registrados en la ciudad, con información sobre el tipo de delito, fecha y lugar y cantidad de víctimas (Perversi 2007, pp. 15-17). A partir de esta información, el

mapa del delito constituye un instrumento de gran valor para evaluar la situación criminal aunque sólo contemple los hechos de autoría desconocida en la jurisdicción de referencia (Behar y Lucilli, 2003).

No obstante, recién en el año 2017 el GCBA publica en el portal BA Data el conjunto de datos sobre criminalidad registrada reflejado en un nuevo mapa del delito, diferente al confeccionado en el año 2002. El Ministerio de Seguridad de la Nación transfiere los datos recabados por las dependencias de la Policía Federal Argentina al Ministerio de Justicia y Seguridad de la ciudad, en el marco de la suscripción del convenio de transferencia progresiva de facultades y funciones de seguridad en todas las materias no federales. Dichos datos se agregan a la base ya existente de la ex Policía Metropolitana con el objeto de armar un repositorio que contenga toda la información policial de la jurisdicción y el mapa del delito.

Este mapa, que contiene en su diseño las experiencias internacionales sobre la implementación de esta herramienta, utiliza datos que refieren a conductas presuntamente delictivas las cuales, posteriormente, pueden ser confirmadas, modificadas en su tipología original, o bien desestimadas como delito. Sin embargo, y a pesar de la normativa vigente, las conductas registradas como delictivas (en forma preliminar a su juzgamiento) pueden ser consideradas valiosas para diagnosticar la problemática de la criminalidad y diseñar e implementar iniciativas que optimicen la asignación de los recursos financieros y humanos disponibles. En este sentido, el mapa se basa en un sistema estadístico dinámico en el cual los hechos registrados se modifican cualitativa o cuantitativamente en la medida en que las fuentes de información utilizadas ratifiquen o rectifiquen los datos.

A pesar de que el mapa del delito constituye una fuente de información fundamental para la confección de estadísticas delictivas que surgen de las denuncias policiales y los registros judiciales, no se utiliza para el análisis predictivo de delitos ni, consecuentemente, para el diseño de políticas de seguridad pública basadas en evidencia. Junto con la situación sanitaria relacionada con la pandemia, la inseguridad continúa siendo una de las principales preocupaciones ciudadanas.

El análisis de los registros criminales resulta prioritario en la prevención del delito. No obstante, en Argentina este tipo de análisis siempre se ha realizado con herramientas

estadísticas descriptivas o deductivas que no reflejan acabadamente las relaciones entre las variables. Para abordar el fenómeno del delito, se requiere de la minería de datos para potenciar el tratamiento de la información criminal y, con ello, predecir tendencias delictivas que permitan diseño de políticas y planes de prevención efectivos.

Capítulo 5: Metodología

5.1 Introducción

Previo al desarrollo de la metodología con la cual se aborda el problema de estudio, es menester definir tres conceptos básicos, a saber: conjunto de datos, modelo y aprendizaje (García Cambronero y Gómez Moreno, 2006, p. 1).

Un conjunto de datos es una colección de números o valores que suelen presentarse de forma tabular y se refiere a un tema específico. Puede dividirse en dos conjuntos, uno de entrenamiento y otro de prueba. El primero se utiliza para analizar y determinar el modelo y contiene el 75% de los datos, mientras que el segundo se aplica para testearlo o estimar el error de generalización con el 25% de los datos restantes. Esta división se obtiene mediante una muestra aleatoria simple.

En segunda instancia, un modelo es una representación de una relación entre variables en los datos, es decir, una descripción de cómo una o más variables se relacionan con otras. Modelar es un proceso en el que una representación abstracta se construye a partir de los datos observados. Una vez que el modelo es creado, puede usarse para predecir el valor de un *output* basándose en los *inputs*. En el marco del análisis predictivo, la minería de datos es el proceso de construir un modelo representativo que se ajuste a los datos observados. Dicho modelo reviste utilidad en dos sentidos: por un lado, predice el *output* basándose en las variables de entrada y, por otro lado, se puede utilizar para comprender la relación entre el *output* y todos los *inputs*. (Kotu y Deshpande, 2015, p. 3).

Por último, y desde un punto de vista técnico, el aprendizaje se puede definir como "el proceso mediante el cual un sistema mejora y adquiere destreza en la ejecución de sus tareas, y tiene la capacidad de poseer inferencia inductiva sobre éstas" (García Cambronero y Gómez Moreno, 2006, p. 2). En ese sentido, el aprendizaje constituye un medio que se emplea para construir determinado modelo a partir de un conjunto de entrenamiento.

Para realizar este trabajo, se utiliza el *software* de minería de datos *Rapidminer Studio* que permite predecir los delitos violentos mediante el encadenamiento de operadores de

entrada y salida, el pre procesamiento de los datos y la visualización a través de un entorno gráfico.

Como se mencionó en el capítulo 2, la minería de datos consiste en un proceso de descubrimiento de conocimiento que abarca diferentes etapas. Como afirma Morales (2003, como se citó en Valenga, 2007, p. 3), abarca diversas fases: la selección de un conjunto de datos sobre el cual realizar un proceso de descubrimiento; la limpieza y el pre procesamiento de los datos, que incluye no sólo el análisis exploratorio sino también el tratamiento de valores ausentes (*missing values*), atípicos o fuera de rango (*outliers*), entre otros; la transformación de los datos al formato requerido por los algoritmos seleccionados, sea mediante la creación o la eliminación de atributos; la selección de la tarea de descubrimiento a realizar, en este caso clasificación, así como de los algoritmos aplicables para dicha tarea; la aplicación del proceso de minería de datos; la interpretación y evaluación de los patrones descubiertos y su presentación mediante técnicas gráficas de visualización.

5. 2. Tipo de estudio

En concordancia con los objetivos enunciados en la introducción, el enfoque del estudio es cuantitativo exploratorio y el tipo de diseño longitudinal.

Se realiza un análisis exploratorio de los *datasets* de delitos publicados en el portal de datos abiertos del GCBA. Creado en 2012, BA Data publica más de 412 conjuntos de datos en formato abierto sobre diversas temáticas como administración pública, educación, cultura y turismo, desarrollo humano, economía y finanzas, medioambiente, movilidad, salud, género, urbanismo y territorio y seguridad. En materia de seguridad, están disponibles los datos sobre delitos correspondientes al período de estudio seleccionado.

Recién a partir del año 2017, se publica el conjunto de los datos sobre la criminalidad registrada. Por consiguiente, los datos utilizados en el presente trabajo corresponden al periodo 2016-2019. El criterio de selección de las dimensiones espacio temporales es utilizar los datos disponibles. Cabe mencionar que los delitos cometidos durante el año 2020 no se incorporan al análisis por motivo de la pandemia, la cual ha provocado algunas distorsiones en los valores consignados que afectan cualquier tipo de predicción.

Los *datasets* originales contienen cuatro tipos de delitos, a saber: homicidios, lesiones, hurtos (sin violencia) y robos (con violencia), de los cuales se selecciona esta última tipología. El *dataset* original utilizado se denomina "Delitos 2019" y suministra información mensual a través de los siguientes atributos: número de identificador, fecha, franja horaria, tipo de delito, subtipo de delito, cantidad registrada, comuna, barrio, latitud y longitud. Los *datasets* "Delitos 2016", "Delitos 2017" y "Delitos 2018", cuyos datos se incorporan en una instancia posterior, poseen idéntica estructura. A continuación, se detalla cada atributo con su descripción así como el tipo de dato:

- Id: identificador de cada delito. Tipo de dato entero.
- Fecha: fecha de comisión del delito. Tipo de dato fecha AAAA-MM-DD.
- Franja_horaria: franja horaria de comisión del delito. Los valores oscilan entre 0 y 23, es decir, cada franja horaria se corresponde a una hora reloj. Tipo de dato entero.
- Tipo_delito: tipo de delito cometido. Puede tomar cuatro valores: homicidio, hurto, lesiones y robo. Tipo de dato polinomial.
- Subtipo_delito: subtipo de delito cometido. Puede tomar cuatro valores: doloso (homicidio), automotor (hurto o robo), no automotor (hurto o robo) y siniestro vial (lesiones). Tipo de dato polinomial.
- Cantidad_registrada: cantidad de delitos registrada en cada franja horaria. Puede tomar distintos valores pero se supone que en una franja horaria con una latitud y longitud específica, sólo puede ocurrir un delito. Tipo de dato entero.
- Comuna: número de comuna en que se cometió el delito. Los valores oscilan entre 1 y 15. Tipo de dato entero.
- Barrio: nombre del barrio en que se cometió el delito. Puede tomar 48 valores: Retiro, San Nicolás, Puerto Madero, San Telmo, Montserrat, Constitución, Recoleta, Balvanera, San Cristóbal, Barracas, La Boca, Nueva Pompeya, Parque Patricios, Almagro, Boedo, Caballito, Flores, Parque Chacabuco, Villa Soldati, Villa Lugano, Villa Riachuelo, Liniers, Mataderos, Parque Avellaneda, Villa Real, Monte Castro, Versalles, Floresta, Vélez Sarsfield, Villa Luro, Villa General Mitre, Villa Devoto, Villa del Parque, Villa Santa Rita, Coghlan, Saavedra, Villa Urquiza, Villa Pueyrredón, Núñez, Belgrano, Colegiales, Palermo, Chacarita, Villa Crespo, La Paternal, Villa Ortúzar, Agronomía y Parque Chas. Tipo de dato polinomial.

- Lat: latitud del lugar donde ocurrió el delito. Tipo de dato real.
- Long: longitud del lugar donde ocurrió el delito. Tipo de dato real.

A partir de los *datasets* mencionados, la Figura 4 exhibe la cantidad de delitos cometidos en la CABA durante el período de estudio con el objetivo de conocer la tendencia de los tipos de hechos delictuales.

Figura 4

Cantidad de tipos de delitos por año en valores absolutos

	Cantidad			
Tipo de delito	2016	2017	2018	2019
Lesiones	8890	9851	10061	10106
Homicidio	289	266	277	198
Hurto	46178	42150	42274	49351
Robo	71226	68297	71121	62829
Total	126583	120564	123733	122484

Como el objetivo es clasificar los delitos, se consideran violentos a los robos mientras que los restantes se los tipifica como no violentos (hurtos, homicidios y lesiones). De este modo, si se unifican los homicios, las lesiones y los hurtos en un conjunto denominado "resto de delitos", se puede apreciar que los robos representan, durante todos los años, más de la mitad de los delitos cometidos en la jurisdicción (Figuras 5 y 6). Para el periodo seleccionado, el porcentaje de robos sobre el total de los delitos denunciados asciende a 56,27% en 2016, 56,65% en 2017, 57,48% en 2018 y 51,3% en 2019.

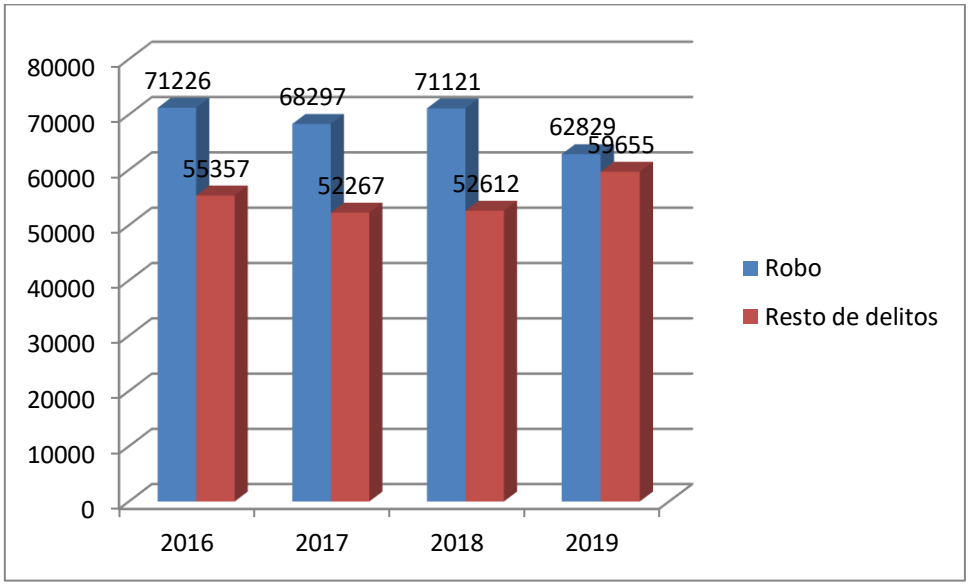
Figura 5

Cantidad de robos y resto de delitos por año en valores absolutos

Tipo de delito	2016	2017	2018	2019
Robo	71226	68297	71121	62829
Resto de delitos	55357	52267	52612	59655
Total	126583	120564	123733	122484

Figura 6

Gráfico de cantidad de robos y resto de delitos por año en valores absolutos



5. 3 Tratamiento de los datos

Los *datasets* originales necesitan ser pre procesados para completar y/o eliminar celdas vacías o valores atípicos, suprimir columnas innecesarias y agregar elementos relevantes. Para ello, se utilizan métodos de extracción y selección de atributos que permiten identificar y suprimir aquellos datos que puedan ser redundantes o irrelevantes. Con relación a la extracción, cada característica nueva es una combinación de los atributos originales; para la selección, se escogen aquellos que brindan información más precisa dependiendo de qué predicción que se quiere realizar. Asimismo, la eliminación de información irrelevante o con ruido reduce el error de los modelos de clasificación.

En este sentido, se procede a eliminar aquellas celdas que no contienen información sobre el barrio en cuestión o sobre la franja horaria en que se comete el delito. Por otro lado, no se encuentran valores atípicos. A continuación, la Figura 7 muestra la nueva cantidad de registros para cada año.

Figura 7

Cantidad de delitos después del tratamiento de los datos

Año	Celdas sin barrio	Celdas sin franja horaria	Total registros
2016	626	3	125954
2017	1841	19	118704
2018	5300	14	118419
2019	692	4	121788

Como se explicita anteriormente, los valores ausentes modifican levemente la cantidad de registros según el tipo de delito (Figuras 8 y 9).

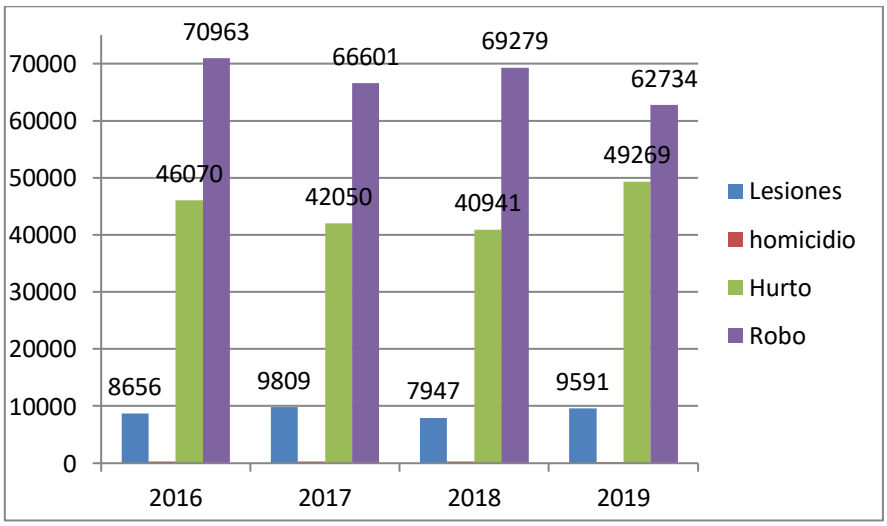
Figura 8

Cantidad de tipos de delitos después del tratamiento de los datos

	Cantidad			
Tipo de delito	2016	2017	2018	2019
Lesiones	8656	9809	7947	9591
Homicidio	265	244	252	194
Hurto	46070	42050	40941	49269
Robo	70963	66601	69279	62734
Total	125954	118704	118419	121788

Figura 9

Gráfico de la cantidad de tipos de delitos después del tratamiento de los datos



A partir de la Figura 10, se puede observar que los robos continúan siendo el tipo de delito predominante en la jurisdicción representando el 56,34% del total para el año 2016; 56,11% para 2017; 58,5% para 2018 y 51,51% para 2019.

Figura 10

Participación relativa de los tipos de delitos por año

	Participación relativa			
Tipo de delito	2016	2017	2018	2019
Lesiones	6.87%	8.26%	6.71%	7.88%
homicidio	0.21%	0.21%	0.21%	0.16%
Hurto	36.58%	35.42%	34.57%	40.45%
Robo	56.34%	56.11%	58.50%	51.51%

A partir del *dataset* "Delitos 2019" obtenido luego del tratamiento de los datos, se calcula el primer modelo denominado línea de base (*baseline*) utilizando *Microsoft Excel*. En este sentido, cualquier modelo seleccionado con posterioridad para realizar las predicciones debe superar el umbral de la línea de base. Para ello, se computa el cociente entre los delitos violentos y el total de los delitos con el objetivo de obtener una primera medida de exactitud.

Para un problema de dos clases, se dice que un conjunto de datos está desbalanceado cuando el número de muestras de la clase mayoritaria es significativamente superior al de la clase minoritaria (García Jiménez, 2010, p. 27). Existen algoritmos de clasificación, como la RL, sensibles a las proporciones de las diferentes clases. Si el conjunto de entrenamiento está desbalanceado, dichos algoritmos suelen favorecer a la clase mayoritaria lo que puede generar métricas de exactitud sesgadas.

Es dable destacar que esta etapa, así como la transformación del conjunto de datos al formato requerido por el algoritmo, resulta de capital importancia para que los patrones descubiertos al finalizar el estudio sean de calidad (Valenga et al., 2007). La calidad de las predicciones depende de la transformación de los atributos del conjunto de datos que se realice previamente. Aquellas que se utilizan frecuentemente consisten en el aumento o disminución de la dimensionalidad, la discretización de atributos numéricos, la numerización de atributos nominales y la normalización.

Con relación al aumento de la dimensionalidad, este se logra mediante la creación de nuevos atributos a partir de los existentes. En el caso de la fecha, el atributo original con formato AAAA-MM-DD brinda escasa información si se lo emplea directamente; no obstante, al crearse los atributos día, mes y día de la semana se logra capturar la misma información de manera más eficiente. Otro ejemplo similar es la creación de los atributos delitos por barrio, construidos a partir de los *datasets* de los años 2016, 2017 y 2018, que reflejan la cantidad de tipos de delitos cometidos por barrio expresada en porcentaje.

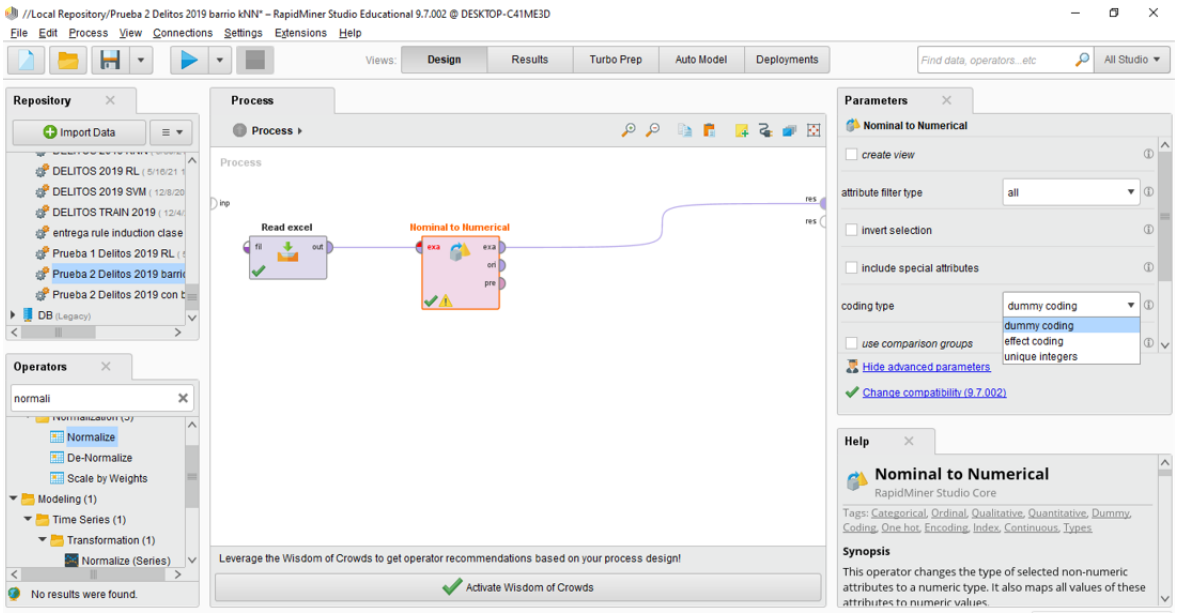
Cabe mencionar que la transformación de atributos mencionada en el párrafo precedente se realiza en las hojas de cálculo de *Microsoft Excel*. Las columnas representan los atributos para cada serie de datos y las filas son un ejemplo de los mismos. Para exportar el archivo al *Rapidminer Studio,* se utiliza el operador *Read Excel*.

Por otra parte, se utiliza la numerización en los casos en que los atributos nominales u ordinales deban convertirse en números. Para los nominales suele utilizarse una representación binaria y para los ordinales suele utilizarse una representación entera. Tal es el caso de la variable objetivo, en la que se reemplazan los valores “si” y “no” por 1 y 0, y del atributo día de la semana, cuyos valores oscilan entre 1 y 7, respectivamente.

Para realizar esta operación en *Rapidminer Studio*, se utiliza el operador *Nominal to Numerical* que tiene por objeto no sólo cambiar los valores de los atributos no numéricos a numéricos, sino que también asigna todos los valores de estos atributos a un tipo numérico. Los atributos numéricos del *dataset* original no sufren modificaciones. Los atributos binarios los convierte en 0 y 1. A través del parámetro tipo de codificación (*coding type*), este operador brinda tres formas de conversión de los atributos, a saber: enteros únicos (*unique_integers*), codificación de efectos (*effect_coding*) y codificación ficticia (*dummy_coding*). La Figura 11 refleja el entorno gráfico de esta descripción.

Figura 11

Operador Nominal to Numerical y sus parámetros



Nota. Salida de *Rapidminer Studio*

Al elegir la opción enteros únicos, el atributo nominal se convierte en un atributo de valor real equidistante. En el caso de la codificación de efectos, se crea un nuevo atributo para todos los valores del atributo nominal excluyendo el grupo de comparación, que es un parámetro obligatorio. En cada ejemplo, el atributo nuevo correspondiente al valor nominal real de ese ejemplo obtiene un valor de 1 y los nuevos atributos restantes un valor de 0. Una variable *dummy*, binaria o ficticia, es aquella que toma valores iguales a 1 o a 0 y que se utiliza para reexpresar variables nominales. En el presente trabajo, se utiliza la codificación ficticia la cual crea un nuevo atributo para todos los valores del atributo nominal. Dicho nuevo atributo que corresponde al valor nominal real de cada ejemplo, obtiene el valor 1 y todos los atributos nuevos restantes obtienen el valor 0.

De esta manera, se agregan los siguientes atributos a la enumeración realizada previamente:

- Dia: día en que ocurrió el delito. Puede tomar valores entre 1 y 30 o 31, dependiendo del mes. Tipo de dato entero.
- Mes: mes en que ocurrió el delito. Puede tomar valores entre 1 y 12, donde 1 representa el mes de enero, 2 el mes de febrero, 3 el mes de marzo, 4 el mes de

abril, 5 el mes de mayo, 6 el mes de junio, 7 el mes de julio, 8 el mes de agosto, 9 el mes de septiembre, 10 el mes de octubre, 11 el mes de noviembre y 12 el mes de diciembre. Tipo de dato entero.

- Dia_ semana: día de la semana en que ocurrió el delito. Puede tomar valores entre 1 y 7, donde 1 representa el día lunes, 2 el día martes, 3 el día miércoles, 4 el día jueves, 5 el día viernes, 6 el día sábado y 7 el día domingo. Tipo de dato entero.
- Delito_violento: indica si el delito cometido es violento (robo) o no violento (delitos restantes). Puede tomar dos valores: 1 en el primer caso y 0 en el segundo. Es la variable objetivo que se quiere predecir (*label*). Tipo de dato binomial.
- Delitos2019_barrio: porcentaje de tipo de delito cometido por barrio en el año de referencia. Tipo de dato real.
- Delitos2018_barrio: porcentaje de tipo de delito cometido por barrio en el año de referencia. Tipo de dato real.
- Delitos2017_barrio: porcentaje de tipo de delito cometido por barrio en el año de referencia. Tipo de dato real.
- Delitos2016_barrio: porcentaje de tipo de delito cometido por barrio en el año de referencia. Tipo de dato real.

Como sostiene Tupiza (2007, como se citó en Flores-Gutiérrez, 2021, p. 44), el análisis espacial constituye una herramienta complementaria para estudiar los hechos delictivos aunque, aisladamente, no refleja la complejidad del fenómeno.

Cabe destacar que, dentro del análisis espacial, el denominado Problema de Unidad Espacial Modificable (PUEM) siempre constituye una limitación metodológica (Gélvez, 2018, p. 81; Linares, 2012, pp. 12-14). Como afirma Openshaw (1984, como se citó en Linares, 2012, pp. 12-13), dicho problema se debe a la creación de unidades espaciales artificiales para estudiar y explicar determinados fenómenos y tiene dos limitantes: por un lado, se encuentra el problema de la escala, propio de considerar agregaciones de unidades geográficas dentro de otras más grandes. Por otro lado, se encuentra el problema de la agregación que surge al emplear distintas unidades del mismo tamaño (Sáenz Vela, 2016, p. 389). Ambas situaciones generan alteraciones en los resultados.

Para intentar reducir el PUEM, no se incluye el *input* "barrio" pero se construyen las variables de entrada denominadas "delito_barrio" que representan, de manera anual, el

porcentaje de tipo de delito –violento o no violento- en el barrio en cuestión. Toda vez que el objetivo del presente trabajo no constituye identificar zonas críticas de delitos violentos –en cuyo caso hubiese sido adecuado incluir los atributos latitud y longitud- sino predecir la ocurrencia de los mismos, se crean estas variables por barrio y no por comuna, dado que el nivel de agregación resultaría mayor, sobredimensionando el problema recientemente descripto.

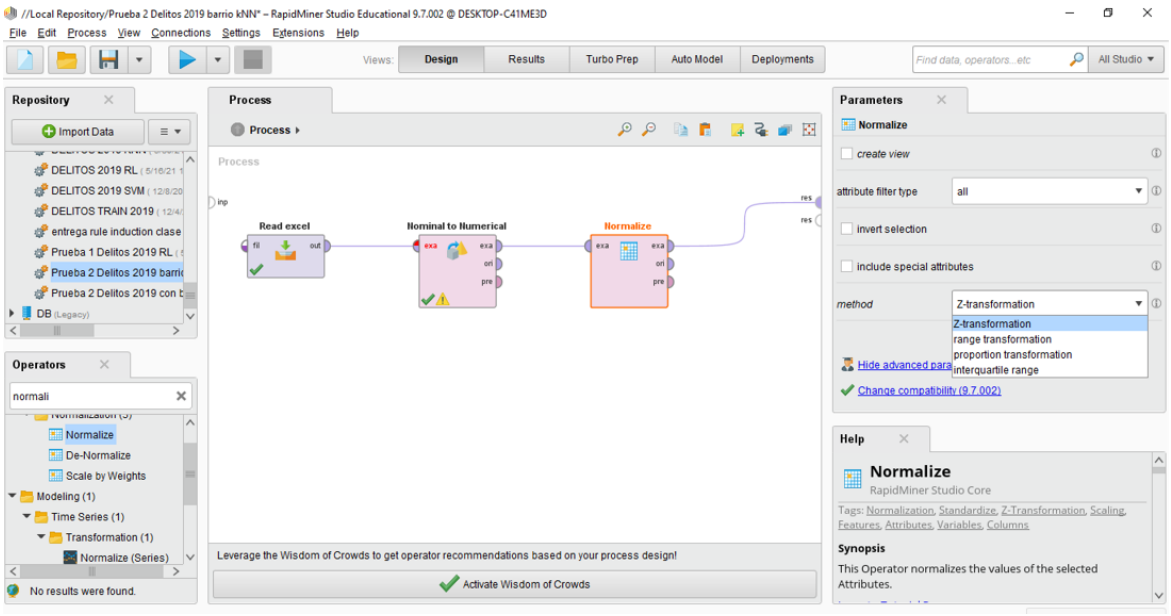
5.4 Aplicación de los modelos de RL y k-NN en *Rapidminer Studio*

Tal como se mencionó en el apartado anterior, la transformación de atributos reviste capital importancia para que el algoritmo elegido arroje una *perfomance* adecuada. Para ello, además del aumento de la dimensionalidad y la numerización de atributos nominales, resulta necesario aplicar la normalización de atributos para los modelos seleccionados.

El operador *Normalize* normaliza los valores de los atributos seleccionados para que se ajusten a un determinado rango. Ajustar el valor del rango resulta una tarea prioritaria cuando los atributos están en diferentes unidades y escalas. Por ejemplo, cuando se utiliza la distancia euclidiana todos los atributos deben tener la misma escala para que la comparación sea válida. El programa proporciona cuatro métodos para llevar a cabo la normalización, saber: transformación *z* (*z-transformation)*, rango intercuantil *(interquartile range)*, transformación de rango *(range transformation)* y transformación de proporción *(proportion transformation)*. En la Figura 12, se puede observar esta descripción.

Figura 12

Operador Normalize y sus parámetros



Nota. Salida de *Rapidminer Studio*

En el presente trabajo, se utiliza la transformación *z* también denominada normalización estadística: se resta de todos los valores la media de los datos y luego se los divide por la desviación estándar. De este modo, la distribución del conjunto de datos tiene una media equivalente a cero y una varianza igual a uno y está menos influenciada por valores atípicos.

Por su parte, el rango intercuantil utiliza el rango intercuartílico definido como la distancia entre los percentiles 25 y 75 (cuartil inferior y superior respectivamente), previo ordenamiento de los datos. Dicho rango se calcula restando el cuartil inferior al superior, correspondiente al percentil 50 o mediana. La fórmula final es el cociente entre la mediana y el mencionado rango. Con relación a la transformación de rango, la misma normaliza todos los valores de atributo a un rango de valores especificado que incluye un mínimo y un máximo. Como los demás valores se escalan, terminan encajando en el rango dado. Finalmente, en la transformación de proporción, cada valor se divide por el valor del atributo completo, dado por la suma de todos los valores de ese atributo.

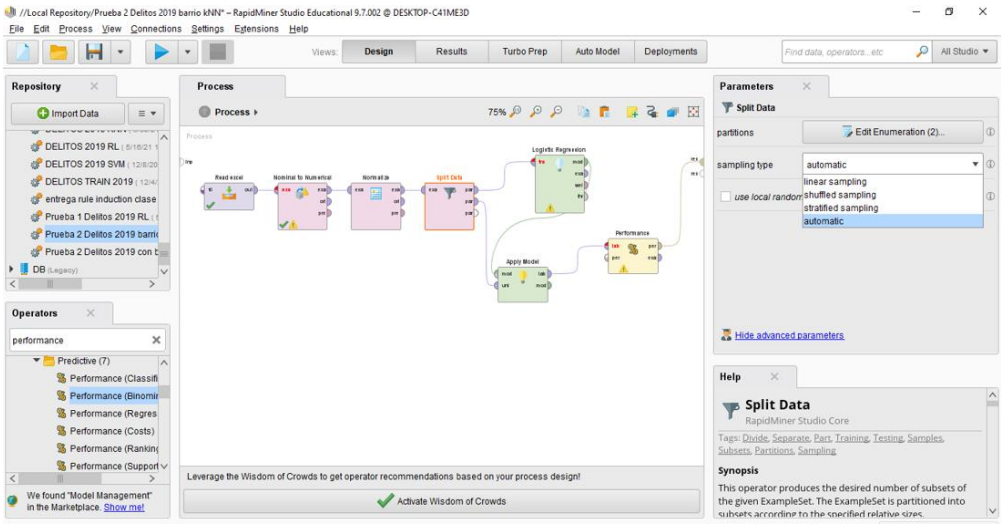
Previamente a la aplicación de los algoritmos seleccionados, resulta necesario dividir el conjunto de datos original para que los modelos puedan “aprender” los datos del conjunto

de entrenamiento. Para ello, se utiliza el operador *Split Data* que produce la cantidad de subconjuntos (particiones) deseados a partir del *dataset* original, es decir, este último se divide de acuerdo con las proporciones especificadas en los parámetros. El operador tiene dos parámetros, a saber: particiones (*partitions*) y tipo de muestreo (*sampling type*). El primero es el más relevante dado que especifica la proporción relativa de cada partición: en este caso se eligió la proporción 0,8 y 0,2. Por lo tanto, el puerto de salida con el 80% de los datos se conecta al operador del modelo elegido (RL o k-NN) y el puerto de salida con el 20% se conecta al operador *Apply Model*. El segundo permite elegir qué tipo de muestreo se quiere utilizar: muestreo lineal (*linear sampling*), aleatorio *(shuffled sampling*), estratificado (*stratified sampling*) y automático (*automatic*). Se optó por este último que utiliza muestreo estratificado si la etiqueta es nominal o, en caso contrario, muestreo aleatorio.

Como se explicitó en el capítulo 2, el objetivo de la aplicación de las técnicas de aprendizaje supervisado consiste en obtener una clasificación binaria de los delitos, según sean o no violentos. En este contexto, la variable objetivo o dependiente toma valor 1 si el delito es violento y 0 sino lo es, y se emplean las variables independientes o predictoras descriptas oportunamente en los apartados 5.2 y 5.3. Como se exhibe en la Figura 13, y mediante la aplicación del operador *Logistic Regression,* se genera un modelo de RL que permite clasificar clases binarias.

Figura 13

Aplicación del modelo RL en Rapidminer Studio

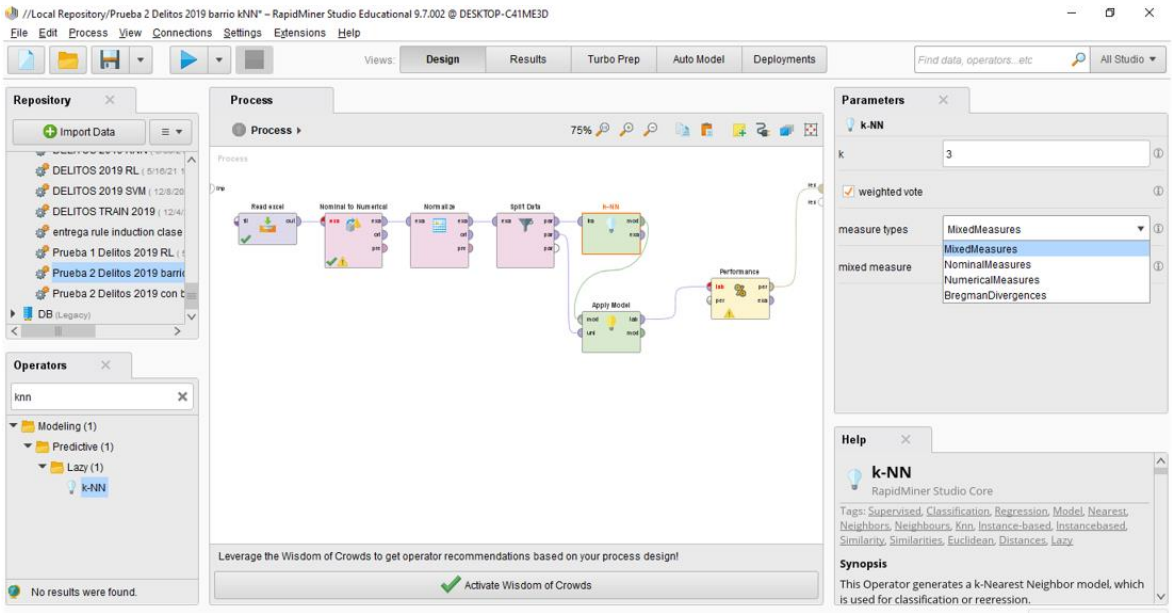


Nota. Salida de *Rapidminer Studio*

A su vez, el operador *k-NN* genera un modelo de k-vecinos más cercanos y se basa en comparar un ejemplo desconocido con los *k* ejemplos de entrenamiento. Como este algoritmo se calcula a partir de métricas de proximidad, las cuales suelen depender de valores absolutos, resulta necesario normalizar los datos previamente. Dentro de los parámetros disponibles, se encuentran distintos tipos de medida (measure_types) para calcular la distancia entre dichos ejemplos: medidas mixtas (*mixed measures*), medidas numéricas (*numerical measures*), medidas nominales (*nominal measures*) y divergencias de Bregman (*Bregman divergences)* En este caso, se selecciona el parámetro medidas numéricas con el objetivo de aplicar la distancia euclidiana, tal como se desprende de la Figura 14.

Figura 14

Aplicación del algoritmo k-NN en Rapidminer Studio



Nota. Salida de *Rapidminer Studio*

Asimismo, el algoritmo k-NN clasifica el ejemplo desconocido por un voto mayoritario de los vecinos encontrados. Si se habilita el parámetro *weighted vote*, los vecinos que tengan una distancia menor al ejemplo que se quiere predecir tienen mayor importancia que aquellos que se encuentran más alejados. Si se desestima el uso de dicho parámetro, todos los vecinos más próximos tienen el mismo peso relativo en la predicción.

Finalmente, el operador *Apply Model* se encarga de accionar el modelo con base en el conjunto de datos de entrada y el operador *Performance Binomial* se utiliza para evaluar el desempeño del modelo predictivo. En esta instancia, se elige el criterio de desempeño que se quiere utilizar, en este caso, la exactitud a través de la matriz de confusión y el área bajo la curva ROC (acrónimo de *Receiver Operating Characteristic* o Característica Operativa del Receptor), llamada comúnmente AUC (acrónimo de *Area Under the Cuve* o Área Bajo la Curva).

5.5. Métricas para la evaluación de los modelos

Existen distintas herramientas disponibles para evaluar la capacidad predictiva de un modelo de clasificación binario, a saber: la matriz de confusión, la curva ROC y el AUC

(Kotu y Deshpande, 2015, pp. 257-259). En el presente trabajo, se utiliza la matriz de confusión para evaluar la *performance* de los modelos. Como se desprende de la Figura 15, las columnas representan el valor real de la variable objetivo mientras que las filas representan el valor predicho de la misma variable.

Figura 15

Matriz de confusión

		Valor Real	
		Positivo	Negativo
Valor predicho	Positivo	Verdadero positivo (VP)	Falso positivo (FP)
	Negativo	Falso negativo (FN)	Verdadero negativo (VN)

En los casos de los VP y los VN, los valores predichos coinciden con el valor real de la variable objetivo. En el primer caso, el valor real es positivo así como la predicción que arroja el modelo. En el segundo, el valor real es negativo y también la predicción. Para los FP y FN, el valor predicho es falso. En el primer caso, el valor real es negativo pero el modelo predice un valor positivo (comúnmente conocido como error de tipo I); en el segundo caso, el valor real es positivo pero el modelo predice un valor negativo (denominado error de tipo II).

De esta manera, la información contenida en la diagonal compuesta por los VP y los VN representa los elementos que han sido clasificados correctamente. Un modelo con una exactitud del 100% es aquel cuya matriz de confusión sólo contiene información en dicha diagonal y elementos iguales a cero en la diagonal opuesta, es decir, FP = FN = 0.

Asimismo, a partir de esta matriz se pueden calcular las siguientes métricas: la exactitud (*accuracy*), la especificidad (*precision*), la sensibilidad (*recall*) y el error. Mientras que la exactitud explica cuántas, de todas las clases, se predicen correctamente, la sensibilidad indica cuántas se predicen acertadamente de todas las positivas. Por su parte, la especificidad refleja qué proporción de positivos reales se condicen con la predicción y el error constituye el complemento de la exactitud. A continuación, se enumeran las respectivas fórmulas:

$$\text{Exactitud} = (VP + VN) / (VP + VN + FP + FN) \quad (11)$$

$$\text{Especificidad} = VP / (VP + FP) \quad (12)$$

$$\text{Sensibilidad} = VP / (VP + FN) \quad (13)$$

$$\text{Error} = 1 - \text{exactitud} \quad (14)$$

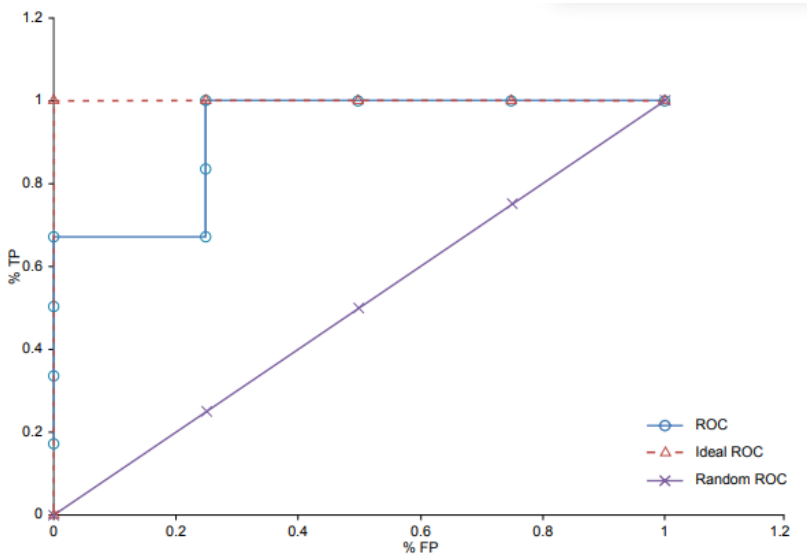
Resulta dable destacar que la sensibilidad es una métrica relevante cuando las clases están desbalanceadas. Tal como se mencionó, los datos están desbalanceados si la proporción de una de las dos clases está sesgada. La solución para este problema consiste en balancear el conjunto de entrenamiento para que las clases estén equilibradas o agregar penalidades sobre las clasificaciones erróneas (Kotu y Deshpande, 2015, pp. 257-259).

En una clasificación binaria, se puede establecer un umbral arbitrario para distinguir entre ejemplos falsos y verdaderos. Al aumentar el valor de dicho umbral, se reduce la cantidad de instancias clasificadas como positivas y se incrementa el número de aquellas clasificadas como negativas. Esto genera una disminución de los VP con el consiguiente aumento de los FN y un aumento de los VN con el correspondiente descenso de los FP. Por lo tanto, las tasas de VP (TVP) y FP (TFP) disminuyen (Musumeci et al, 2018, p. 1401).

Para distintos valores de umbrales, la curva ROC traza la TVP o la sensibilidad en el eje vertical y la TFP o (1- especificidad) en el eje horizontal. Esta curva constituye una representación gráfica de la sensibilidad frente a la especificidad según varía el umbral de discriminación, es decir, explicita los intercambios entre los VP y los FP. Un modelo predictivo con buen desempeño genera una curva ROC por encima de la diagonal del plano (TFP, TVP), por ello, los puntos ubicados por debajo de la diagonal representan resultados de clasificación pobres. El modelo de predicción perfecta se sitúa en la esquina superior izquierda o punto (0,1); con una sensibilidad del 100% (no existe ningún FN) y una especificidad del mismo valor (ningún FP). Esta coordenada en el espacio ROC recibe la denominación de clasificación perfecta (Figura 16).

Figura 16

Curva ROC



Nota. Tomado de *Predictive Analytics and Data Mining. Concepts and Practice with Rapidminer Studio* (p. 262), por V. Kotu, y B. Deshpande, 2015, Elsevier.

Cabe mencionar que, si bien la curva ROC es una herramienta gráfica eficiente para evaluar el desempeño de un clasificador, el AUC es una medida numérica que sintetiza la *performance* del algoritmo independientemente del umbral que se haya elegido (Musumeci et al., 2018, p. 1401).

5.6. Selección del modelo: validación cruzada y problemas de sobreajuste y subajuste de los datos

Los métodos de remuestreo (*resampling methods*) o de validación permiten estimar la capacidad predictiva de uno o más modelos cuando se aplican a nuevas observaciones, utilizando solamente el conjunto de datos de entrenamiento. Como el error medido en la muestra de entrenamiento es un indicador deficiente para realizar una generalización del resultado del modelo, este último se ajusta empleando un subconjunto de observaciones del conjunto de entrenamiento y se evalúa con las observaciones restantes. Este proceso es iterativo y los resultados obtenidos se agregan para luego promediarse, permitiendo compensar las desviaciones que puedan surgir por la manera en que se distribuyeron las observaciones.

Entre los métodos de remuestreo más utilizados, cabe destacar el *bootstrap* y la validación cruzada (*cross-validation*). La técnica de *bootstrap* consiste en obtener, al menos de forma aproximada, la distribución de un estadístico utilizando la información que se deriva de una sola muestra (y sus réplicas). Por su parte, la validación permite evaluar el desempeño o rendimiento de un clasificador o, en su defecto, decidir a partir de una serie de clasificadores cuál es el mejor. A partir de la división aleatoria de la muestra en dos submuestras, una de entrenamiento y otra de prueba, permite obtener un error de predicción relativamente realista. El mejor clasificador es aquel cuya tasa de error proporciona el menor error de generalización (Sayeh y Bellier, 2014). Existen diversos procedimientos para aplicar este proceso, entre los que cabe mencionar la validación cruzada aleatoria, los métodos *Leave-One-Out Cross-Validation* (LOOCV), *k-fold cross-validation* y *repeated k-fold cross-validation* (Refaeilzadeh et al., 2009).

En la validación cruzada aleatoria, la división de los conjuntos de entrenamiento y prueba se realiza de manera aleatoria y el valor obtenido surge del promedio aritmético de los resultados en cada una de las divisiones. A pesar de que la partición de los datos de entrenamiento y prueba no depende del número de iteraciones, no se puede asegurar que todas las muestras sean elegidas como parte de alguno de los conjuntos y, además, pueden existir muestras que sean elegidas en más de una iteración.

Por otro lado, el método *Leave-One-Out Cross-Validation* (LOOCV) es un caso particular del *k-fold* en el que en cada iteración se utilizan todos los datos excepto una única observación con la cual, además, el modelo se prueba. Si bien el error que se obtiene suele ser muy bajo, el costo computacional es elevado dado que se utilizan todas las observaciones lo que, además, puede generar problemas de sobreajuste de los datos (Refaeilzadeh et al., 2009).

En el caso de *k-fold cross validation* (validación cruzada con *k* iteraciones), el conjunto de datos original se divide aleatoriamente en *k* subconjuntos mutuamente excluyentes, cada uno aproximadamente del mismo tamaño (Han et al., 2012, pp. 370-371). El modelo se entrena *k* veces utilizando cada uno de los *k* subconjuntos para la validación y los (k -1) restantes para el entrenamiento (Hastie et al., 2009, pp. 241-243). Este proceso se repite durante *k* iteraciones, alternando con cada uno de los subconjuntos de prueba disponibles

y, por último, se calcula la media aritmética de los resultados de cada iteración. En este sentido, la validación cruzada sólo estima de manera efectiva el error promedio.

Finalmente, la técnica *repeated k-fold cross-validation* resulta similar a la descripta en el párrafo precedente, pero repite el proceso de validación cruzada *n* veces (Refaeilzadeh et al., 2009).

Cuando el objetivo de la clasificación es predecir un *output* y conocer la precisión del modelo, el método con *k* iteraciones garantiza que la evaluación de los resultados sea independiente de la partición entre el conjunto de datos de entrenamiento y el de prueba. Ahora bien, cabe preguntarse qué valor debe elegirse para el parámetro configurable *k*.

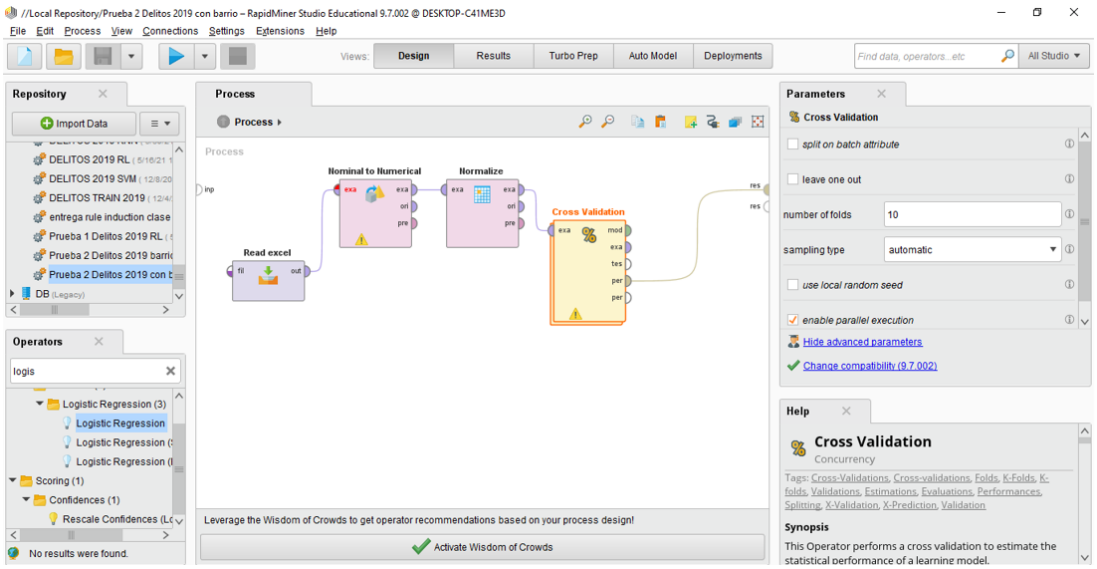
En el caso en que *k* = N, el estimador de validación cruzada es casi insesgado para el error de predicción esperado, pero es plausible que tenga alta varianza dado que los N conjuntos de entrenamiento son muy similares entre sí. Asimismo, la carga computacional resulta considerable pues se requieren N aplicaciones del método elegido para realizar la predicción (Hastie et al., 2009, pp. 241-243). Para valores de *k* pequeños, la validación cruzada tiene menor varianza. No obstante, el sesgo podría convertirse en un problema, dependiendo de cómo varía el desempeño del método a medida que varía el tamaño del conjunto de entrenamiento. Resulta evidente que el rendimiento del clasificador mejora a medida que aumenta el tamaño de los datos de entrenamiento (Hastie et al., 2009, pp. 241-243).

Existe consenso en la literatura sobre el valor que este parámetro debe adoptar en la práctica: suele utilizarse *k* = 10, es decir, para calcular la predicción de un modelo se utiliza repetidamente el 90% de los datos y se prueba su precisión en el 10% restante. Si el conjunto de entrenamiento es lo suficientemente grande y ese 10% de los datos tiene una distribución similar a las instancias etiquetadas, se obtiene una estimación confiable (Refaeilzadeh et al., 2009).

Tal como se muestra en la Figura 17, el operador *Cross Validation* realiza una validación cruzada dividiendo aleatoriamente el conjunto de entrenamiento y prueba y realizando una evaluación del modelo. Para realizar esta operación, resulta preciso eliminar el operador *Split Data*.

Figura 17

Operador Cross Validation con 10 iteraciones

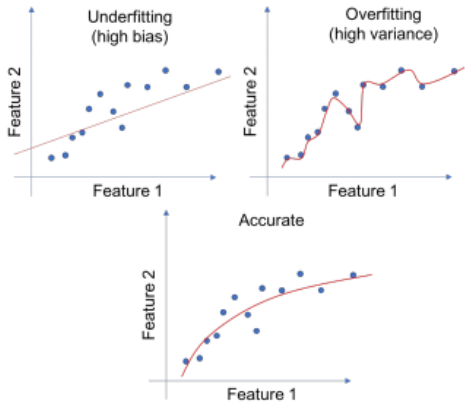


Nota. Salida de *Rapidminer Studio*

Por otra parte, la selección del modelo predictivo tiene dos aristas: el sobreajuste (*overfitting*) y el subajuste (*underfitting*) de los datos. El sobreajuste sucede cuando el modelo elegido se torna demasiado complejo para el conjunto de entrenamiento utilizado. El modelo se ajusta de sobremanera a los datos, incluyendo los ruidos y los valores atípicos y, en consecuencia, el resultado brinda predicciones poco exactas para el conjunto de prueba. Por el contrario, el subajuste ocurre cuando se seleccionan modelos que no logran captar las características relevantes de los datos (Musumeci, et al., 2018, p. 1388). La Figura 18 exhibe las diferencias entre ambos conceptos.

Figura 18

Subajuste, sobreajuste y exactitud



Nota. Tomado de "An overview on application of machine learning techniques in optical networks" (p. 1388), por F. Musumeci et al., 2018, *IEEE Communications Surveys & Tutorials, 21*(2).

Si existe sobreajuste, el error medido en el conjunto de prueba es alto y en el conjunto de entrenamiento es bajo. En el caso de subajuste, tanto el error medido en el conjunto de entrenamiento como en el conjunto de prueba suele ser alto (Musumeci, et al., 2018, p. 1388).

En el capítulo siguiente, se presentan los resultados obtenidos para ambos modelos así como las métricas relacionadas a sus desempeños: la exactitud, la sensibilidad, la especificidad, el error de predicción y la AUC. Asimismo, se incorporan las salidas de *Rapidminer Studio* con las matrices de confusión y, con relación a la RL, se detallan los valores de los coeficientes que explican la importancia de cada atributo seleccionado en función de la variable que se quiere predecir. Posteriormente, se elaboran cuadros comparativos para facilitar la exposición. Por último, se detallan los resultados de la validación cruzada y se recalculan las matrices de confusión y las AUC para los parámetros establecidos.

Capítulo 6: Resultados obtenidos

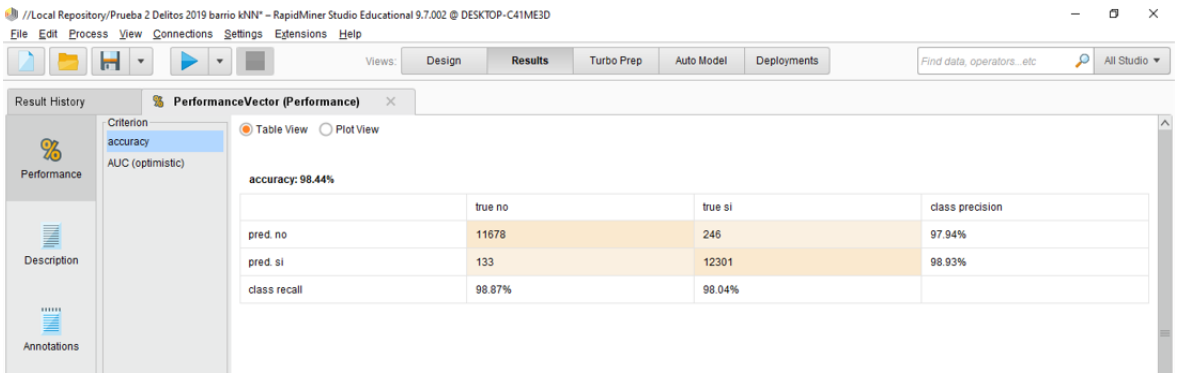
6.1 Resultados de las métricas para evaluar los modelos RL y k-NN

A partir del *dataset* "Delitos 2019" obtenido luego del tratamiento de los datos, se calcula el primer modelo denominado línea de base (*baseline*) utilizando *Microsoft Excel*. Para ello, se computa el cociente entre los delitos violentos y el total de los delitos con el objetivo de obtener una primera medida de exactitud. Para el año 2019, esta métrica asciende a 51,51% (62734/121788), lo que también demuestra que las clases están balanceadas. Asimismo, cualquier modelo predictivo seleccionado con posterioridad debe superar el valor de la línea de base.

Por su parte, el modelo de RL para todos los atributos, excluyendo latitud y longitud, barrio[10] y delitos por barrio en 2019, arroja una exactitud del 98,44%, con la matriz de confusión correspondiente a la Figura 19.

Figura 19

Matriz de confusión para la RL



Nota. Salida de *Rapidminer Studio*

Tal como se definió previamente, los VP (12301) y los VN (11678) representan los elementos que han sido clasificados correctamente. Asimismo, puede comprobarse que la cantidad de FP (133) es menor que la de FN (246), lo que sugiere que el costo de las predicciones de clases incorrectas no es uniforme.

[10] La información del barrio está contenida en los atributos delitos por barrio, por ello excluirlo no representa una pérdida de información.

Exactitud = (12301+11678)/(12301+11678+246+133) = 0.98444043 = 98,44%

Analizando los resultados verticalmente, se puede observar que de los delitos violentos 12301 fueron clasificados como tales (VP), mientras que 246 son los denominados FN o aquellos que el modelo clasifica incorrectamente. A partir de estos valores, se puede calcular la métrica sensibilidad como el cociente entre los VP y la suma de los VP y los FN.

Sensibilidad (delito violento) = 12301/(12301+246) = 0.98039372 = 98,04%

A partir de la lectura horizontal de la matriz, del total que se predice como delito violento el modelo indica que 12301 corresponden a esta tipología (VP) y 133 no (FP). Idéntico razonamiento aplica a la clase restante. La métrica calculada a partir de los valores mencionados se denomina especificidad y asciende a:

Especificidad (delito violento) = 12301/(12301+133) = 0.98930352 = 98,93%

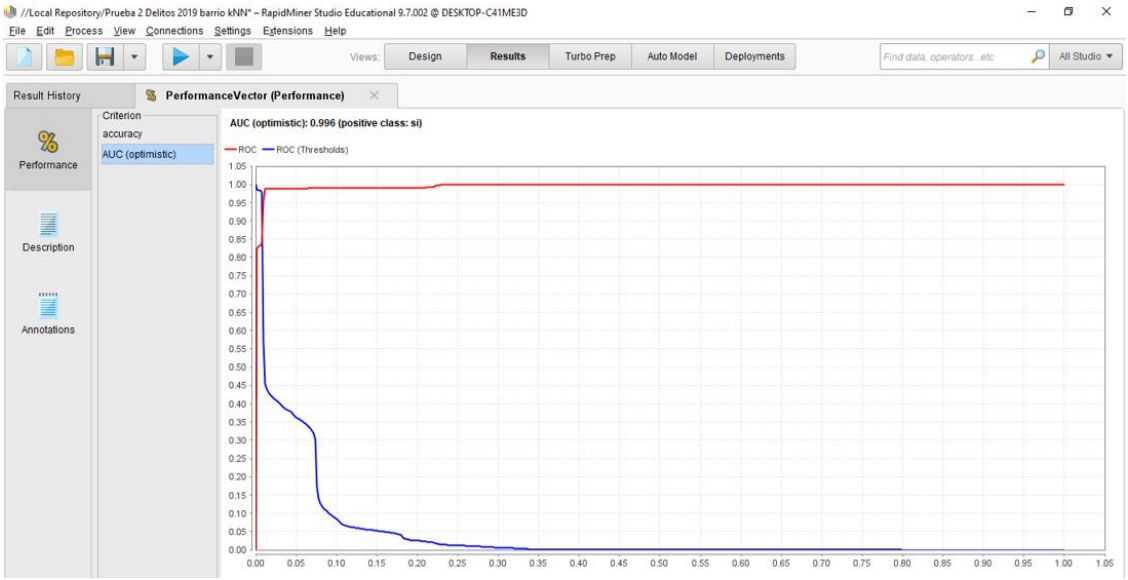
Por su parte, el error de predicción, entendido como el completo de la exactitud, arroja el siguiente valor:

Error = 1 – exactitud = 1- 0.98444043 = 0.01555957 = 1,56%

Con relación al AUC, la Figura 20 exhibe un resultado de 0,996.

Figura 20

Resultado de la AUC para la RL

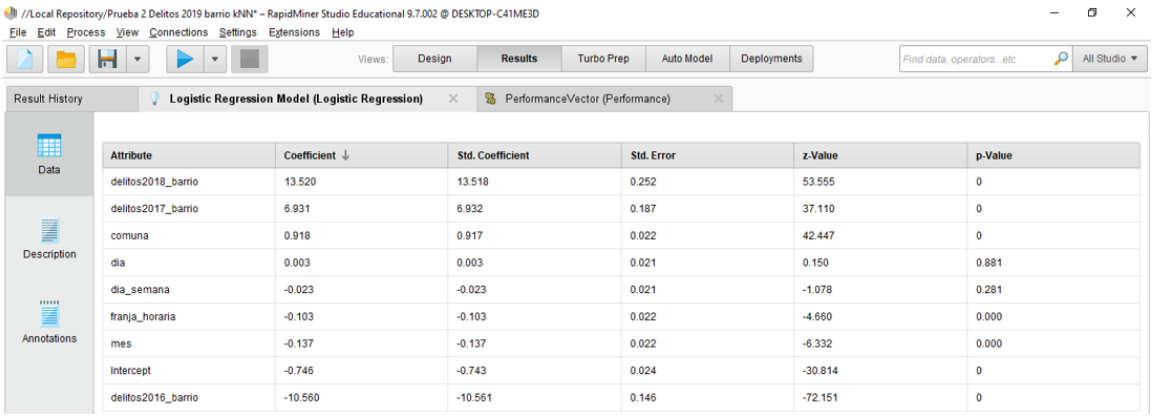


Nota. Salida de *Rapidminer Studio*

Por otra parte, y a partir de la Figura 21, se pueden observar los coeficientes de la RL.

Figura 21

Coeficientes de la RL



Attribute	Coefficient	Std. Coefficient	Std. Error	z-Value	p-Value
delitos2018_barrio	13.520	13.518	0.252	53.555	0
delitos2017_barrio	6.931	6.932	0.187	37.110	0
comuna	0.918	0.917	0.022	42.447	0
dia	0.003	0.003	0.021	0.150	0.881
dia_semana	-0.023	-0.023	0.021	-1.078	0.281
franja_horaria	-0.103	-0.103	0.022	-4.660	0.000
mes	-0.137	-0.137	0.022	-6.332	0.000
Intercept	-0.746	-0.743	0.024	-30.814	0
delitos2016_barrio	-10.560	-10.561	0.146	-72.151	0

Nota. Salida de *Rapidminer Studio*

En este sentido, el atributo “delitos 2018_barrio” con un coeficiente de 13,52 constituye la variable más relevante para definir si un delito es o no violento. El segundo coeficiente, y con una diferencia numérica considerable, alcanza un valor de 6,931 y representa la incidencia de los delitos cometidos por barrio en el año 2017. En tercer lugar, la variable

independiente que influye en la predicción es el número de comuna en la que se registra el hecho delictivo.

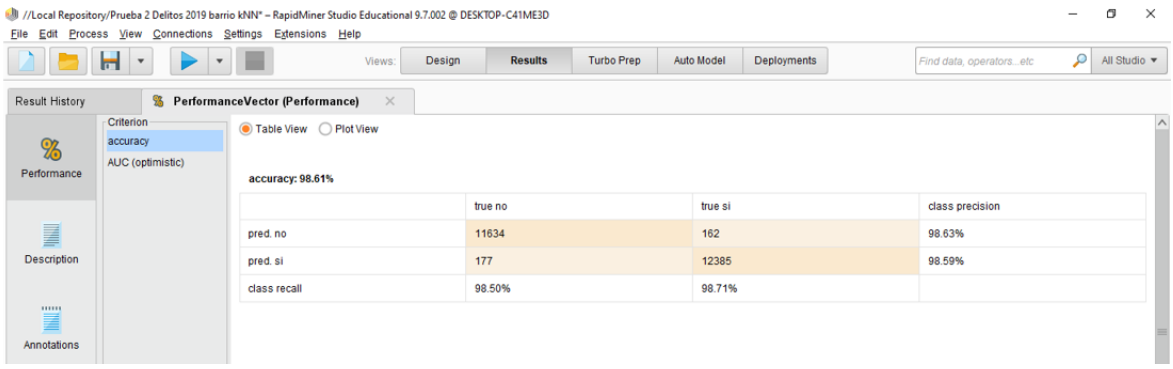
En el caso de las variables con coeficiente negativo, la más significativa es “delitos 2016_barrio” con -10,56, lo que significa que el porcentaje de tipo de delito por barrio en el año 2016 no explica la ocurrencia de delitos violentos. Se aplica el mismo razonamiento para los coeficientes siguientes, a saber: mes con -0.137, franja horaria con -0.103 y día de la semana con -0,023.

Asimismo, es dable destacar que las variables elegidas como predictoras alcanzan un valor-p (*p-value)* igual a 0 o menor a 0,5 lo que demuestra relevancia en el estudio realizado. La única excepción la representa el atributo “día” con valor de 0,881, que se condice con el valor del coeficiente que apenas alcanza el 0,003.

Utilizando los mismos atributos que para la RL, el algoritmo k-NN para *k* = 3 y *weighted vote*, arroja una exactitud de 98,61% con la matriz de confusión que se exhibe en la Figura 22.

Figura 22

Matriz de confusión para los k-NN



Nota. Salida de *Rapidminer Studio*

Tal como se definió previamente, los VP (12385) y los VN (11634) representan los elementos que han sido clasificados correctamente. Asimismo, y en contraposición con el modelo anterior, puede comprobarse que los FP (177) son más costosos que los FN (162).

Exactitud = (12385+11634)/(12385+11634+177+162) = 0.9860826 = 98,61%

Analizando los resultados verticalmente puede observarse que, de los delitos violentos, 12385 fueron clasificados como tales (VP), mientras que 162 son los denominados FN o aquellos que el modelo clasifica incorrectamente. De este modo, la sensibilidad arroja el siguiente valor:

Sensibilidad (delito violento) = 12385/(12385+162) = 0.98708855 = 98,71%

A partir del análisis horizontal de la matriz, del total que se predice como delito violento el modelo indica que 12385 corresponden a esta tipología (VP) y 177 no (FP). Idéntico razonamiento aplica a la clase restante. A partir de los valores mencionados, la especificidad alcanza el siguiente porcentaje:

Especificidad (delito violento) = 12385/(12385+177) = 0.98590989 = 98,59%

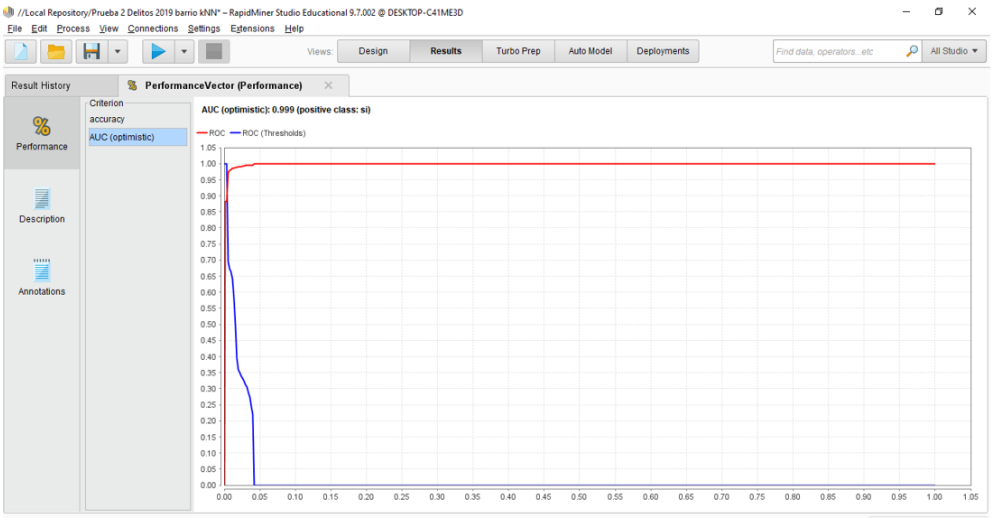
Por su parte, el error de predicción asciende a:

Error = 1 – exactitud = 1- 0.9860826 = 0.0139174 = 1,39%

Con relación al AUC, la misma alcanza un valor de 0,995 como se desprende de la Figura 23.

Figura 23

AUC para los k-NN



Nota. Salida de *Rapidminer Studio*

Para comparar las métricas de ambos modelos, se confeccionan las Figuras 24 y 25 con el objetivo de simplificar la exposición de los resultados obtenidos.

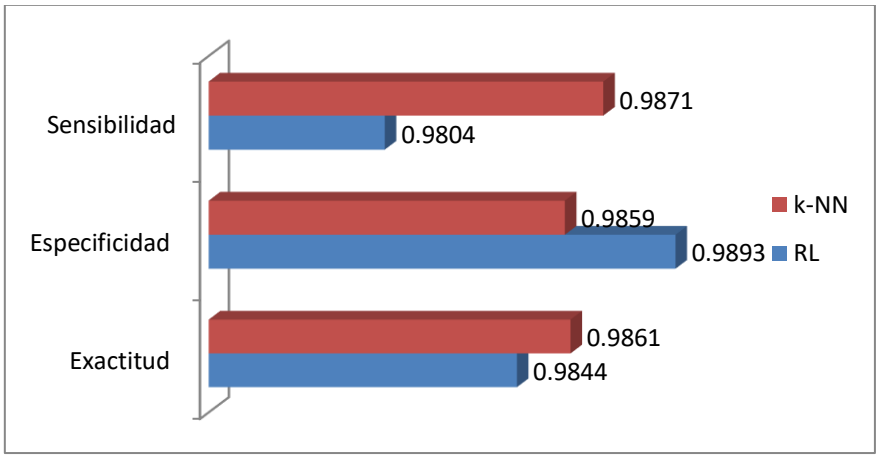
Figura 24

Comparación de las métricas de la RL y los k-NN

Método	Exactitud	Especificidad	Sensibilidad
RL	0.9844	0.9893	0.9804
k-NN	0.9861	0.9859	0.9871

Figura 25

Comparación gráfica de las métricas de la RL y los k-NN



A partir de las Figuras 26 y 27, se pueden comparar los porcentajes de las clasificaciones correctas y los errores de predicción para cada modelo.

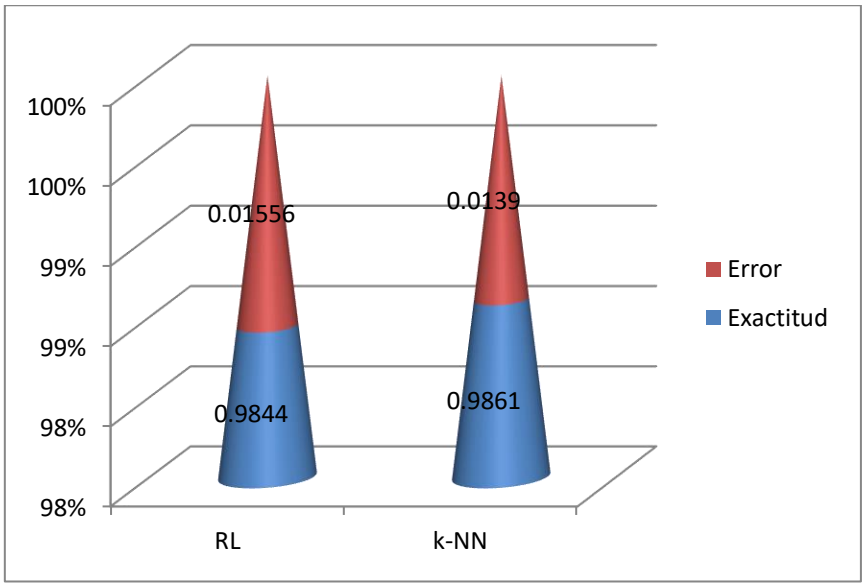
Figura 26

Comparación de la exactitud y el error de cada modelo

Método	RL	k-NN
Exactitud	0.9844	0.9861
Error	0.01556	0.0139

Figura 27

Comparación gráfica de la exactitud y el error de cada modelo

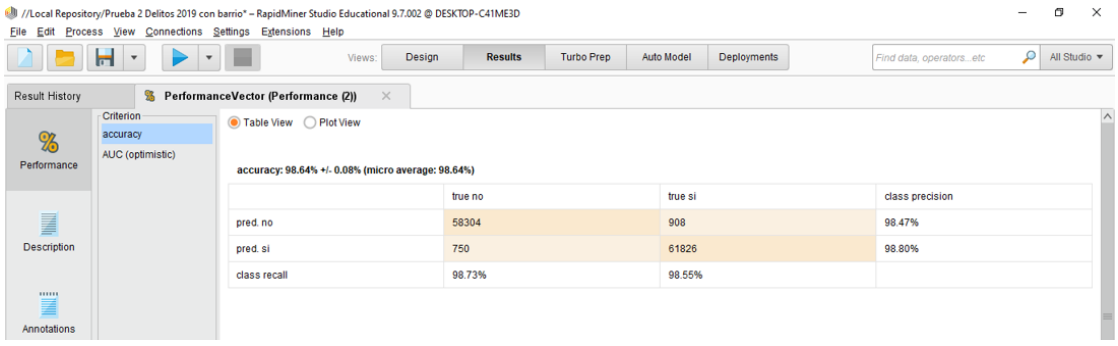


6.2 Resultados de la validación cruzada

Al realizar la validación cruzada en *Rapidminer Studio* para el modelo k-NN, con *k* = 3 y 10 iteraciones, se obtiene que la exactitud alcanza un 98,64% con una desviación de +/- 0,08%. Las Figuras 28 y 29 exhiben la matriz de confusión y la curva AUC que asciende a 0,999 sin ningún tipo de desviación.

Figura 28

Matriz de confusión de la validación cruzada con los k-NN



Nota. Salida de *Rapidminer Studio*

Figura 29

AUC de la validación cruzada con los k-NN

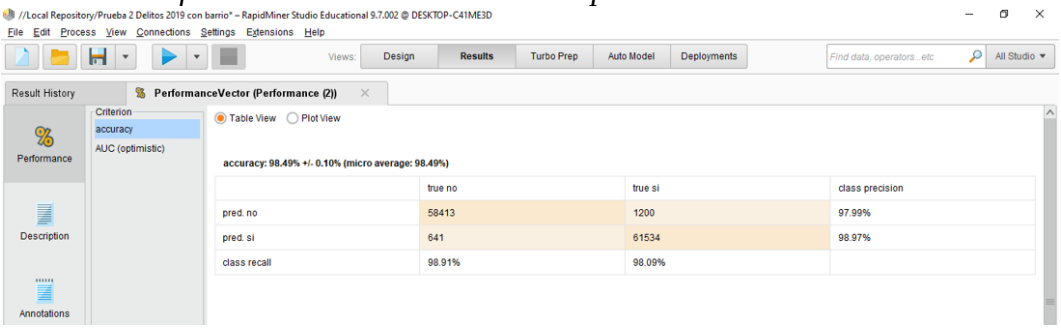
Nota. Salida de *Rapidminer Studio*

Si la validación cruzada se realiza con 5 iteraciones, la exactitud alcanza un 98,58 % con una desviación de 0,04+/- % mientras que el AUC arroja el mismo valor que con 10 iteraciones. Se puede observar que, a medida que aumenta la cantidad de iteraciones, se incrementa la exactitud del modelo pero también su desviación.

Para el caso de la RL, la validación cruzada se realiza con 10 iteraciones y la exactitud alcanza un 98,49% con una desviación de +/- 0,1%. Por su parte, el AUC asciende a 0,996. Estos resultados se pueden observar en las Figuras 30 y 31.

Figura 30

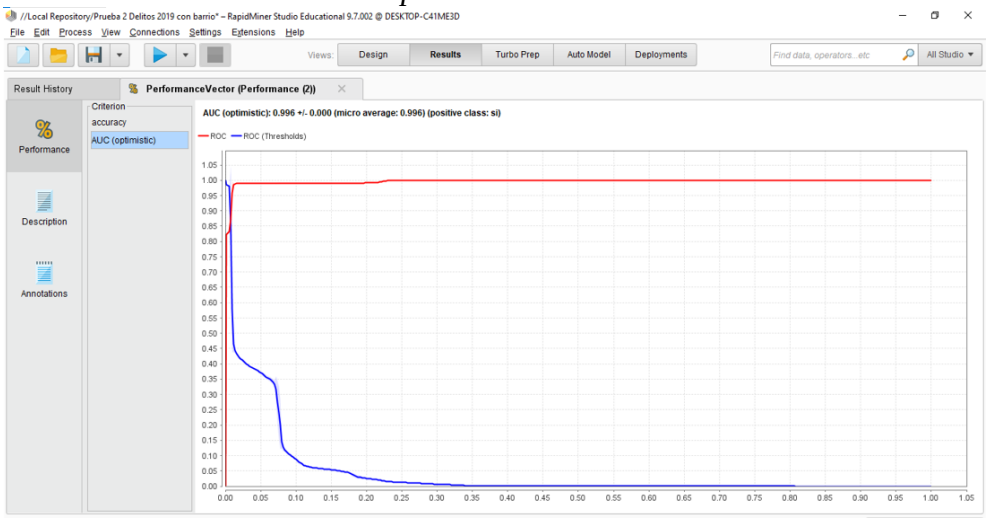
Matriz de confusión de la validación cruzada para la RL



Nota. Salida de *Rapidminer Studio*

Figura 31

AUC de la validación cruzada para RL



Nota. Salida de *Rapidminer Studio*

Para este modelo, si la validación cruzada se realiza con 5 iteraciones, la exactitud alcanza un 98,48% con una desviación de +/- 0,08% y el AUC asciende a 0,996, valor que no sufre modificaciones respecto del cálculo original.

De los resultados obtenidos, se desprende que el algoritmo k-NN presenta una *performance* superior a la RL para predecir la ocurrencia de delitos violentos en CABA: la exactitud de los modelos alcanzan, con los parámetros especificados precedentemente, un 98,61% (AUC = 0,995) y un 98,44% (AUC=0,996) respectivamente. El resultado de la validación cruzada con 10 iteraciones utilizando los k-NN tiene una exactitud del 98,64% con una desviación de +/- 0,08% y el AUC alcanza un 0,999. Manteniendo la cantidad de iteraciones pero aplicando la RL, se obtiene una exactitud del 98,49% con una desviación de +/- 0,1% y el AUC asciende a 0,996.

Capítulo 7: Conclusiones y posibles líneas de investigación

7.1 Algunas conclusiones y futuras líneas de investigación

En las últimas décadas, el acceso a datos abiertos y el surgimiento de nuevas tecnologías basadas en internet han posibilitado la difusión de los modelos predictivos como técnicas idóneas para cuantificar los riesgos delictivos. A partir del cálculo de la probabilidad de ocurrencia de delitos violentos, la aplicación de los modelos de clasificación RL y k-NN permite optimizar la identificación de oportunidades y amenazas, crear un marco para la toma de decisiones informadas, perfeccionar los métodos de seguimiento y monitoreo y mejorar la prevención de hechos delictivos.

La gran cantidad de información circulante y las múltiples variables que intervienen para predecir la ocurrencia de los delitos, justifica la utilización de herramientas más potentes que los métodos estadísticos convencionales. En este sentido, las técnicas propias del aprendizaje automático brindan sistemas de medición de riesgos delictuales más precisos y personalizados. Al basarse en un aprendizaje continuo y automático, disminuye el margen de error y evalúa permanentemente patrones y desvíos de manera más eficiente que las herramientas estadísticas tradicionales.

Con la creación del portal BA Data, y para promover el acceso a la información pública, el GCBA pone a disposición de los ciudadanos múltiples conjuntos de datos (entre ellos, el de delitos) con una amplia gama de temáticas para que el público pueda reutilizarlos. Para ello, resulta necesario que continúe invirtiendo en infraestructura tecnológica que posibilite progresivamente que todos los sistemas de datos gubernamentales sean interoperables. De este modo, se pueden alcanzar objetivos de diversa índole que abarcan desde la optimización de los procesos de entrega de información hasta el aumento de la confianza de la ciudadanía en la gestión del gobierno. Fomentar una política de datos abiertos que incluya información sobre todas las áreas de interés público, así como disponibilizar los datos en formatos que sean sencillos de usar, debe continuar siendo una prioridad en la agenda del GCBA.

Resulta fundamental, para llevar a cabo esta tarea, contar con bases de datos confiables y actualizadas que permitan diseñar políticas públicas adecuadas al territorio en el que se

aplican, que sean flexibles y puedan contener el contexto cambiante y las nuevas formas de delincuencia. Al utilizar *datasets* dinámicos, todo nuevo conjunto de datos que se agregue permite no sólo una mejora con relación a la evaluación de riesgos sino también la identificación de riesgos emergentes o cambios en el contexto. Por eso, los datos constituyen un pilar prioritario en la gestión de riesgos. Asimismo, el GCBA debería fomentar no sólo una cultura de intercambio de información, tanto al interior de su sistema como con sistemas externos, sino también procesos de colaboración y transparencia que posibiliten integrar todo el reservorio de datos de la jurisdicción para tener un diagnóstico más preciso que permita describir el fenómeno del delito en su totalidad.

En el GCBA, los procesos de recopilación, registro y almacenamiento de datos continúan siendo obsoletos y esto no se debe únicamente a la falta de sistemas tecnológicos. Las múltiples fuentes de información disponibles para evaluar la actividad delictiva (encuestas de victimización, registros administrativos policiales y judiciales; datos del registro civil, estadísticas confiables sobre el nivel de ingreso, el nivel educativo formal, entre otras) no pueden ser unificadas y estandarizadas con un criterio homogéneo. Sumado a lo antedicho, las bases de datos de delitos publicadas contienen pocos atributos y no representan la totalidad de los tipos delictivos. La inexistencia de ciertos datos o su falta de disponibilidad se puede deber a diversos factores, que incluyen desde el desconocimiento sobre el uso de los datos hasta la falta de voluntad política para que estén disponibles.

En el marco de la gobernanza, los datos son activos que los gobiernos deben gestionar. Por ello, resulta preciso diseñar un marco normativo que establezca derechos y responsabilidades en la toma de decisiones relacionadas con el uso de datos y algoritmos. También, debe contemplar dimensiones como la privacidad, la seguridad y la protección de los datos de los ciudadanos para evitar robustecer sesgos e inequidades preexistentes o, al menos, reducirlas a su mínima expresión. Una solución factible consiste en la conformación de equipos interdisciplinarios de trabajo que detecten sesgos intrínsecos o de contexto de los datos, de cara al diseño de políticas públicas de seguridad que, al tiempo que busquen reducir los delitos existentes contemplen las implicancias sociales, éticas, políticas y económicas del manejo de información pública.

Pensando en futuras líneas de investigación, y en el marco del estudio realizado por Cong et al. (2015), la clasificación en los algoritmos como k-NN mejora significativamente si, a

las características de entrada, se le aplica una transformación lineal. La clave radica en desarrollar modelos que aprendan de funciones de distancia como un problema de optimización, a partir de restricciones que se obtienen de las instancias de aprendizaje.

Asimismo, podría resultar de interés aplicar otros métodos de clasificación en el conjunto de datos de delitos y evaluar la exactitud de las predicciones. Esto incluye la incorporación de técnicas de aprendizaje no supervisado, como el *clustering*. También, resulta plausible incorporar nuevos atributos e investigar su impacto en el desempeño de los distintos modelos predictivos.

En síntesis, este trabajo permite vislumbran la importancia del uso de datos para el diseño de políticas públicas, tradición que no parece estar extendida en el ámbito de gobierno, no solo en el área de seguridad. La subestimación o la subutilización de los datos para el armado de programas públicos suele ser un factor silenciado en la explicación de los fracasos de las políticas. Y también una excusa su falta de actualización o de interoperabilidad entre sistemas. Para utilizar datos y actualizarlos, es necesario que las políticas se diseñen con herramientas que permitan absorber el dinamismo del contexto e incorporar los cambios que se suceden en el ámbito donde son aplicadas. El uso de datos y la aplicación de modelos de predicción no es una garantía de éxito en el desarrollo de las políticas, pero sí la forma más adecuada de gestionar riesgos.

Referencias bibliográficas

Arshad Zaidi, S.M., Chandola V., Allen, M., Sanyal, J., Stewart, R., Bhaduri, B. y McManamay, R. (2018). Machine learning for energy-water nexus: challenges and opportunities. *Big Earth Data*, *2*(3), 228-267. https://doi.org/10.1080/20964471.2018.1526057

Avenburg, A, Penna, F. y Yankelevich, D. (12 de mayo de 2021). *Sobre la validez de la evidencia*. Fundar. https://www.fund.ar/publicacion/sobre-la-validez-de-la-evidencia/

Ayos, E. J. (2014). ¿Una política democrática de seguridad? Prevención del delito, políticas sociales y disputas en el campo conformado en torno a la "inseguridad" en la Argentina (2000-2010). *Revista del CLAD Reforma y Democracia*, (58), 167-200. https://www.redalyc.org/articulo.oa?id=357533690006

Bandekar, S.R. y Vijayalakshmi, C. (2020). Design and analysis of machine learning algorithms for the reduction of crime rates in India. *Procedia Computer Science, 172*, 122–127. https://doi.org/10.1016/j.procs.2020.05.018

Bazzano, M. M. y Pol, L. (9-10 de diciembre de 2010). *Condiciones de producción de las estadísticas criminales en Argentina* [Presentación en papel].VI Jornadas de Sociología de la Universidad Nacional de La Plata, La Plata, Buenos Aires, Argentina.

Behar, A. M. y Lucilli, P. (2003). *Mapa del delito de la Ciudad Autónoma de Buenos Aires* [Presentación en papel]. III Jornadas de Jóvenes Investigadores. Universidad de Buenos Aires, Buenos Aires, Argentina.

Bell, T. B., Ribar, G. S. y Verichio J. (17-18 de mayo de 1990). *Neural nets versus logistic regression: A comparison of each model's ability to predict commercial bank failures* [Presentación en papel]. X Simposio sobre Problemas de Auditoría. Deloitte y Touche/Universidad de Kansas, Kansas, Estados Unidos.

Bellet, A., Habrard, A. y Sebban, M. (2013). *A Survey on Metric Learning for Feature Vectors and Structured Data*. https://arxiv.org/pdf/1306.6709.pdf

Beltrame, F. (2011). Seguridad ciudadana y nuevas estrategias de control del delito en Argentina. *URVIO, Revista Latinoamericana de Estudios de Seguridad,* (9), 102-112. https://www.redalyc.org/articulo.oa?id=552656555007.

Beltrame, F. (2013). La conformación de la inseguridad como cuestión social y las nuevas estrategias de control del delito en Argentina. *Sociológica, 29* (80), 189-208. https://www.redalyc.org/articulo.oa?id=305029973006

Bharati, A. y Sarvanaguru, R.A.K. (2018). Crime prediction and analysis using machine learning. *International Research Journal of Engineering and Technology*, 5(9), 1037–1042. https://www.irjetnet/archives/V5/i9/IRJET-V5I9192.pdf

Bogomolov, A., Lepri, B., Staiano, J., Oliver, N., Pianesi, F. y Pentland, A. (12 – 16 de noviembre de 2014). *Once Upon a Crime: Towards Crime Prediction from*

Demographics and Mobile Data [Presentación en papel]. XVI Congreso Internacional de Interacción Multimodal, Estambul, Turquía.

boyd, D., y Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society*, *15*(5), 662 –679. http://dx.doi.org/10.1080/1369118X.2012.678878

Breiman, L. (2001). Random forests. *Machine Learning*, *45*, 5-32. https://link.springer.com/article/10.1023/a:1010933404324

Cadena Urzúa, P. y Letelier Saavedra, L. (2018). Factores determinantes de los Delitos de Mayor Connotación Social en la Región Metropolitana. Análisis en base a un modelo de regresión logística. *Revista Política criminal*, *13*(26), 1170-1189.: http://www.politicacriminal.cl/Vol_13/n_26/Vol13N26A14.pdf

Cánovas-García, F., Alonso-Sarría, F., Gomariz-Castillo, F. y Oñate-Valdivieso, F. (2017). Modification of the random forest algorithm to avoid statistical dependence problems when classifying remote sensing imagery. *Computers & Geosciences*, *113*, 1-11. https://www.sciencedirect.com/science/article/pii/S0098300416303909?via%3Dihub

Cerro, A.M. y Meloni, O. (1999). *Análisis económico de las políticas de prevención y represión del delito en la Argentina*. Eudecor.

Chandrasekar, A., Raj, A. S. y Kumar, P. (2015). Crime Prediction and Classification in San Francisco City. http://cs229.stanford.edu/proj2015/228_report.pdf

Chen, M., J. Han y Yu, P. S. (1996). Data mining: An overview from database perspective. *IEEE Transactions on Knowledge and Data Engineering*, *8*(6), 866 –883. https://doi.org/10.1109/69.553155

Chen, H., Atabakhsh, H., Petersen, T., Schroeder, J., Buetow, T., Chaboya, L., O'Toole, C., Chau, M., Cushna, T., Casey, D. y Huang, Z. (18-21 de mayo 2003). *COPLINK: Visualization for Crime Analysis* [Presentación en papel]. Conferencia nacional anual sobre investigación en gobierno digital, Boston, Estados Unidos.

Chen, H., Chung, W., Qin, Y., Xu, J. J., Wang, G., Zheng, R. y Atabakhsh. H. (2003). *Crime Data Mining: An Overview and Case Studies* [Presentación en papel]. Conferencia nacional anual sobre investigación en gobierno digital, Boston, Estados Unidos.

Chen, H; Chung, W; Xu, JJ; Wang, G; Qin y Chau, M. (2004). Crime data mining: A general framework and some examples. *IEEE Computer Society*, *37*(4), 50-56. . https://doi.org/10.1109/MC.2004.1297301d

Chen, P., Yuan, H.Y. y Shu, X.M. (18-20 de octubre de 2008). F*orecasting crime using the ARIMA model* [Presentación en papel]. V Conferencia Internacional sobre Sistemas Difusos y Descubrimiento del Conocimiento, Shandong, China.

Chinchilla M.L y Vorndran, D. (2018). *Seguridad ciudadana en América Latina y el Caribe: Desafíos e innovación en gestión y políticas públicas en los últimos 10 años*. Banco Interamericano de Desarrollo.

https://publications.iadb.org/publications/spanish/document/Seguridad-ciudadana-en-America-Latina-y-el-Caribe.pdf

Chioda, L. (2016). *Fin a la violencia en América Latina: una mirada a la prevención desde la infancia a la edad adulta* [Sinopsis]. Banco Mundial. https://openknowledge.worldbank.org/handle/10986/2592

Christodoulou, P., Decker, S., Douka, A.V., Komopoulou, C., Peristeras, V., Sgagia, S., Tsarapatsanis, V. y Vardouniotis, D. (3-5 de septiembre de 2018). *Data Makes the Public Sector Go Round* [Presentación en papel]. XVII Conferencia International sobre Gobierno Electrónico, Krems, Austria.

Clifton, C. y Marks, D. (1996). *Security and Privacy Implications of Data Mining* [Presentación en papel]. ACM SIGMOD Workshop sobre Data Mining y Descubrimiento del Conocimiento, Montreal, Canadá.

Código Penal (CPen). Ley 11.179 de 1921. Artículo 164. 30 de septiembre de 1921 (Argentina).

Cong, B.N., Pérez, J.L.R. y Morell, C. (2015). Aprendizaje supervisado de funciones de distancia: estado del arte. *Revista Cubana de Ciencias Informáticas*, *9*(2), 14-28. https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=1014

Cover, T. y Hart, P (1967). Nearest neighbor pattern classification. *IEEE Transactions on Information Theory*, *13*(1), 21-27. http://dx.doi.org/10.1109/TIT.1967.1053964

Cramer, J.S. (2002). The origins of Logistic Regression. *Tinbergen Institute Discussion Paper TI 2002-119/4*. http://dx.doi.org/10.2139/ssrn.360300

Cranor, L., Rabin, T., Shmatikov, V., Vadhan, S. y Weitzner, D. (2016). Towards a Privacy Research Roadmap for the Computing Community. *Computing Community Consortium*. https://arxiv.org/ftp/arxiv/papers/1604/1604.03160.pdf

Crespo, F. A. (2017). Una mirada a la desigualdad social y la violencia delictiva en Venezuela. *Revista Criminalidad*, *59*(2), 65-80. http://www.scielo.org.co/pdf/crim/v59n2/1794-3108-crim-59-02-00065.pdf

Dammert, L. (2000). *Violencia Criminal y Seguridad Pública en América Latina: la Situación de Argentina*. CEPAL. https://www.cepal.org/es/publicaciones/5978-violencia-criminal-seguridad-publica-america-latina-la-situacion-argentina

Dammert, L. y Arias, P. (2007). El desafío de la delincuencia en América Latina: Diagnóstico y respuestas de política. En L. Dammert y L. Zúñiga (Ed), *Seguridad y Violencia: desafíos para la ciudadanía* (1ª ed., pp. 21-66). FLACSO.

Dey, A. (2016). Machine learning algorithms: a review. *International Journal of Computer Science and Information Technologies*, *7*(3), 1174-1179. http://ijcsit.com/docs/Volume%207/vol7issue3/ijcsit2016070332.pdf

Domínguez, P. (2020). La delincuencia y la justicia en una sociedad desigual. En M. Busso y J. Messina (Eds.), *La crisis de la desigualdad: América Latina y el Caribe en la encrucijada* (pp. 220-247). Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/La-crisis-de-la-desigualdad-America-Latina-y-el-Caribe-en-la-encrucijada.pdf

Dorofee, A., Walker, J., Alberts, C., Higuera, R., Murphy, R. y Williams, R. (1996). *Continuous Risk Management Guidebook***.** Software Engineering Institute, http://jodypaul.com/SWE/ContinuousRiskManagement.pdf

Estévez, E. E. (2014). Reformando la inteligencia policial en la provincia de Buenos Aires. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (15), 71-84. https://revistas.flacsoandes.edu.ec/urvio/article/view/1589

Fajnzylber, P., Lederman, D. y Loaiza, N. (2002). Inequality and violent crime. *Journal of Law and Economics, 45*(1)-, 1-39. https://doi.org/10.1086/338347

Fayyad, U., Piatetsky-Shapiro, G. y Smyth, P. (2-4 de agosto de 1996). Knowledge Discovery and Data Mining: Towards a Unifying Framework [Presentación en papel]. II Conferencia Internacional sobre Descubrimiento del Conocimiento y Minería de datos, Portland, Oregon, Estados Unidos.

Flores-Gutiérrez, S. (2021). Análisis espacial del delito callejero en Ciudad de México, 2018. *Quivera Revista de Estudios Territoriales*, (*23*)1, 25-47. https://quivera.uaemex.mx/article/view/15072

Focás, B. (2018). Miedo al crimen, prevención del delito y narcotráfico: desafíos para las políticas públicas de seguridad ciudadana en América Latina. Entrevista a Lucía Dammert. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (22), 102-108. http://dx.doi.org/10.17141/urvio.22.2018.3183

Frühling, H. (2012). *La eficacia de las políticas públicas de seguridad ciudadana en América Latina y el Caribe. Cómo medirla y cómo mejorarla*. Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/La-eficacia-de-las-pol%C3%ADticas-p%C3%BAblicas-de-seguridad-ciudadana-en-Am%C3%A9rica-Latina-y-el-Caribe-Como-medirla-y-como-mejorarla.pdf

García Jiménez, V. (2010). *Distribución de clases no balanceadas: métricas, análisis de complejidad y algoritmos de aprendizaje*. [Tesis de Doctorado, Universitat Jaume I]. Repositorio UJI.

García Cambronero, C. y Gómez Moreno, I. (2006). *Algoritmos de aprendizaje: KNN & KMEANS. Inteligencia en Redes de Telecomunicación*. http://www.it.uc3m.es/jvillena/irc/practicas/08-09/06.pdf

Garland, D. (2005). *La cultura del control. Crimen y orden social en la sociedad contemporánea* (Trad. M. Sozzo). Gedisa. (Trabajo original publicado en 2001).

Gélvez, J. D. (2018). ¿Cuáles determinantes se relacionan con la percepción de inseguridad? Un análisis estadístico y espacial para la ciudad de Bogotá. *D. C. Revista Criminalidad*, *61*(1), 69-84. http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S1794-31082019000100069&lng=en&nrm=iso&tlng=es

Gobierno de la Ciudad de Buenos Aires (s.f.). *Delitos*. https://data.buenosaires.gob.ar/dataset/delitos

González-Zapata, F. y Heeks, R. (2015). The Multiple Meanings of Open Government Data: Understanding Different Stakeholders and their Perspectives. *Government Information Quarterly*, *32*(4), 441-452. http://dx.doi.org/10.1016/j.giq.2015.09.001

Grimmelikhuijsen, S., Porumbescu, G., Hong, B. y Im, T. (2013). The Effect of Transparency on Trust in Government: A Cross-National Comparative Experiment. *Public Administration Review, 73*(4), 575-586. http://www.jstor.org/stable/42003079

Guerrero Agripino, L. F. (2007). Seguridad pública y prevención del delito en el Estado social de derecho. Especial comentario a la trascendencia de la educación. *Díkaion, revista de fundamentación jurídica, (16)*, 251-272. https://dialnetunirioja.es/servlet/articulo?codigo=2562421

Gupta, A., Dengre, V., Kheruwala, H.A. y Shah, M. (2020). *Comprehensive review of text-mining applications in finance*. *Journal of Financial Innovation*, *6*(1), 1–25. https://doi.org/10.1186/s40854-020-00205-1

Hagendorff, T. (2020). The Ethics of AI Etics: An Evaluation of Guidelines. *Revista Minds & Machines*, *30*(1), 99–120. https://doi.org/10.1007/s11023-020-09517-8

Hall, P., Park, B. U. y Samworth, R. J. (2008). Choice of neighbor order in nearest-neighbor classification. *The Annals of Statistics*, *36*(5), 2135-2152. http://www.jstor.org/stable/25464706

Han, J., Kamber, M. y Pei, J. (2012). Classification: Basic Concepts. En J. Han, M. Kamber y J. Pei (Eds.), *Data Mining: Concepts and Techniques* (3ª ed., pp. 327-392). Morgan Kaufmann. http://myweb.sabanciuniv.edu/rdehkharghani/files/2016/02/The-Morgan-Kaufmann-Series-in-Data-Management-Systems-Jiawei-Han-Micheline-Kamber-Jian-Pei-Data-Mining.-Concepts-and-Techniques-3rd-Edition-Morgan-Kaufmann-2011.pdf

Hand, D. J. (1998). Data mining: statistics and more? *The American Statistician*, *52*(2), 112-118. https://storm.cis.fordham.edu/~gweiss/selected-papers/data-mining-and-statistics-hand.pdf

Hastie, T., Tibshirani, R. y Friedman, J. (2009). Model Assessment and Selection. En T. Hastie, R. Tibshirani y J. Friedman (Eds.), *The elements of statistical learning* (2ª ed., pp. 219-260). Springer. https://web.stanford.edu/~hastie/Papers/ESLII.pdf

Höchtl, J., P. Parycek y R. Schöllhammer (2016). Big data in the policy cycle: Policy decision making in the digital era. *Journal of Organizational Computing and Electronic Commerce, 26*(1), 147-169. https://doi.org/10.1080/10919392.2015.1125187

Hossain, S., Abtahee, A., Kashem, I., Hoque, M. y Sarker, I.H. (2020). Crime prediction using spatio-temporal data. En N. Chaubey, S. Parikh y K. Amin (Eds.), *Computing Science, Communication and Security*, *1235*, 277-289. Springer. https://doi.org/10.1007/978-981-15-6648-6_22

Instituto Nacional de Estadística y Censos (2018). *Encuesta Nacional de Victimización 2017*. Ministerio de Economía. https://www.indec.gob.ar/indec/web/Nivel4-Tema-4-27-137

Instituto Nacional de Justicia. (s.f.). *Real-Time Crime Forecasting Challenge Posting*. Departamento de Justicia de Estados Unidos. https://nij.ojp.gov/funding/real-time-crime-forecasting-challenge-posting

Iqbal, R., Murad, M. A., Mustapha, A., Panahy, P. H. y Khanahmadliravi, N. (2013). An Experimental Study of Classification Algorithms for Crime Prediction. *Indian Journal of Science and Technology, 6*(3), 1-7. https://doi.org/10.17485/ijst/2013/v6i3.6

Jaitman, L. y Keefer, P. (2017). ¿Por qué es importante la estimación de los costos del crimen? Una agenda de investigación para apoyar las políticas de prevención del delito en la región. En L. Jaitman (Ed.), *Los costos del crimen y de la violencia: nueva evidencia y hallazgos en América Latina y el Caribe* (pp. 1-17). Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/Los-costos-del-crimen-y-de-la-violencia-Nueva-evidencia-y-hallazgos-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Jaitman, L. y Torre, I. (2017). Estimación de los costos directos de la violencia. En L. Jaitman (Ed.), *Los costos del crimen y de la violencia: nueva evidencia y hallazgos en América Latina y el Caribe* (pp. 21-52). Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/Los-costos-del-crimen-y-de-la-violencia-Nueva-evidencia-y-hallazgos-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Janssen, M., Konopnicki, D., Snowdon, J.L. y Adegboyega, O. (2017). Driving Public Sector Innovation Using Big and Open Linked Data (BOLD). *Information Systems Frontiers, 19,* 189-195. https://doi.org/10.1007/s10796-017-9746-2

Jha K., Doshi A., Patel P. y Shah M. (2019). A comprehensive review on automation in agriculture using artificial intelligence. *Artificial Intelligence in Agriculture, 2,* 1–12. https://doi.org/10.1016/j.aiia.2019.05.004

Jha, P., Jha, R. y Sharma, A. (2019). Behavior analysis and crime prediction using big data and machine learning. *International Journal of Recent Technology and Engineering, 8*(1), 461-468. https://www.ijrte.org/wp-content/uploads/papers/v8i1/A3493058119.pdf

Kessler, G. (2009). *El sentimiento de inseguridad. Sociología del temor al delito*. Siglo XXI.

Kessler, G. (9-10 de diciembre de 2010). *Delito, sentimiento de inseguridad y políticas públicas* [Presentación en papel]. Jornadas de Sociología de la Universidad Nacional de La Plata, La Plata, Argentina.

Khatri, V. y Brown, C. V. (2010). Designing Data Governance. *Communications of the ACM, 53*(1), 148-152. https://doi.org/10.1145/1629175.1629210

Kim, S., Joshi, P., Kalsi, P. S., y Taheri, P. (1-3 de noviembre de 2018). *Crime Analysis Through Machine Learning* [Presentación en papel]. Novena Conferencia Anual de Tecnología de la Información, Electrónica y Comunicaciones Móviles, Vancouver, Canadá.

Koontz, W. L. G. (2017). Analysis and Prediction of Call For Service Data**.** *National Criminal Justice Reference Service (NCJRS).* https://www.ojp.gov/pdffiles1/nij/grants/251177.pdf

Kotu, V. y Deshpande, B. (2015*). Predictive Analytics and Data Mining. Concepts and Practice with Rapidminer Studio*. Elsevier.

Kounadi, O., Ristea, A. y Araujo, A. (2020). A systematic review on spatial crime forecasting. *Crime Sci, 9*(7). https://doi.org/10.1186/s40163-020-00116-7

Kuehn, K. y Salter, L. (2020). Assessing Digital Threats to Democracy, and Workable Solutions: A Review of the Recent Literature. *International Journal of Communication, 14*, 2589-2610. https://ijoc.org/index.php/ijoc/article/view/12959/3082

Lammerant, H. y Hert, P. (2016). Predictive profiling and its legal limits: Effectiveness gone forever. En B. van der Sloot, D. Broeders, y E. Schrijvers (Eds.), *Exploring the boundaries of big data* (Vol. 32, pp. 145-173). https://research.tilburguniversity.edu/en/publications/predictive-profiling-and-its-legal-limits-effectiveness-gone-fore

Larson, J., Mattu, S., Kirchner, L. y Angwin, J. (23 de mayo de 2016). *How We Analyzed the COMPAS Recidivism Algorithm*. *Propublica*. https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

Lee, Y., SooHyun, O. y Eck, J. E. (2017). A Theory-Driven Algorithm for Real-Time Crime Hot Spot Forecasting. *National Criminal Justice Reference Service (NCJRS).* https://www.ojp.gov/pdffiles1/nij/grants/251179.pdf

Ley 2593 de 2007. Creación del Sistema de Información para la Prevención Comunitaria del Delito y la Violencia (SIPREC). 06 de diciembre de 2007. B.O. No. 2875.

Ley 5.688 de 2016. Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires. 17 de noviembre de 2016. B.O. No. 5030.

Linares, S. (2012). Dificultades metodológicas al medir la segregación: el problema del tablero de ajedrez y de la unidad espacial modificable. *Revista Geografía y Sistemas de Información Geográfica*, 4(4), 10-22.

https://www.academia.edu/21078501/Dificultades_metodol%C3%B3gicas_al_medir_la_segregaci%C3%B3n_el_problema_del_tablero_de_ajedrez_y_de_la_unidad_espacial_modificable

Lorenc Valcarce, F. (2013). Estado, policías *y* criminalidad*:* seguridad pública *y* seguridad privada en la Argentina actual. *Revista POSTData*, *18*(1), 11-49. http://www.revistapostdata.com.ar/2013/04/estado-policias-y-criminalidad-seguridad-publica-y-seguridad-privada-en-la-argentina-actual-federico-lorenc-valcarce/

Manovich, L. (2012). Trending: The promises and the challenges of big social data. En M. K. Gold (Ed.), *Debates in the Digital Humanities*. University of Minnesota Press. https://doi.org/10.5749/minnesota/9780816677948.003.0047

Masiello, B., y Whitten, A. (22-24 de marzo de 2010). *Engineering Privacy in an Age of Information Abundance* [Presentación en papel]. Series de Simposios de Primavera. Association for the Advancement of Artificial Intelligence, Stanford, California, Estados Unidos.

McClendon, L. y Meghanathan, N. (2015). Using Machine Learning Algorithms to Analyze Crime Data. *Machine Learning and Applications: An International Journal (MLAIJ), 2*(1), 1–12. https://doi.org/10.5121/mlaij.2015.2101.

Meiliana, M., Trisnawarman, D. y Choirul Imam, M. (2020). Prediction Analysis of Criminal Data Using Machine Learning. *IOP Conference Series Materials Science and Engineering, 852*. https://iopscience.iop.org/article/10.1088/1757-899X/852/1/012164/pdf

Metcalf, J., Keller, E.F. y boyd, D. (23 de mayo de 2016). Perspectives on Big Data, Ethics, and Society. *Data & Society*. https://datasociety.net/library/perspectives-on-big-data-ethics-and-society/

Mohler, G. y Porter, M. D. (2017). Rotational grid, PAI-maximizing crime forecasts. *National Criminal Justice Reference Service (NCJRS).* https://www.ojp.gov/pdffiles1/nij/grants/251203.pdf

Musumeci F., Rottondi C., Nag A., Macaluso I., Zibar D., Ruffini M. y Tornatore, M. (2018). An overview on application of machine learning techniques in optical networks. *IEEE Communications Surveys & Tutorials, 21*(2), 1383-1408. https://doi.org/10.1109/COMST.2018.2880039.

Naciones Unidas (20–27 de Abril de 2020a). *Comprehensive strategies for crime prevention towards social and economic development* [Presentación en papel]. XIV Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Kyoto, Japón.

Naciones Unidas (20–27 de Abril de 2020b). *Seminario 1. Prevención del delito de base empírica: estadísticas, indicadores y evaluaciones en apoyo de prácticas eficaces* [Presentación en papel]. XIV Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Kyoto, Japón.

Naik B., Mehta A. y Shah M. (2020). Denouements of machine learning and multimodal diagnostic classification of Alzheimer's disease. *Visual Computing for Industry, Biomedicine, and Art, 3*, 1-18. https://doi.org/10.1186/s42492-020-00062-w

Nelder, J.A., y Wedderburn, R. (1972). Generalized linear models. Journal of the Royal Society. *Journal of the Royal Statistical Society, 135*(3), 370-384. https://www.jstor.org/stable/2344614

Observatorio de Seguridad Ciudadana. (s.f.). *Encuesta Nacional de Victimización*. http://www.seguridadciudadana.org.ar/estadisticas/datos-a-nivel-subnacional/victimizacion-y-percepcion

Oficina de las Naciones Unidas contra la Droga y el Delito (2010). *Manual para encuestas de victimización.* https://www.unodc.org/documents/data-and-analysis/Crime-data-EGM-Feb10/Manual_Victimization_Spanish_030210.pdf

Ordóñez, H., Cobos, C. y Bucheli, V. (2020). Modelo de machine learning para la predicción de las tendencias de hurto en Colombia. *Revista Ibérica de Sistemas e Tecnologías de Información (RISTI), (E29),* 494–506. https://www.proquest.com/docview/2394537974?pq-origsite=gscholar&fromopenview=true

Organización Internacional de Normalización. (2010). *Gestión de riesgos* (31000). https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Ortíz Freuler, J. e Iglesias, C. (2018). *Algoritmos e inteligencia artificial en Latinoamérica. Un estudio de implementaciones por parte de gobiernos en Argentina y Uruguay*. World Wide Web Foundation. http://webfoundation. org/docs/2018/09/WF_AI-in-LA_Report_Spanish_Screen_ AW.pd

Parekh P., Patel S., Patel N. y Shah M. (2020). Systematic review and meta-analysis of augmented reality in medicine, retail, and games. *Visual Computing for Industry, Biomedicine, and Art*, 3, 1-20. https://doi.org/10.1186/s42492-020-00057-7

Pathak, A. N., Sehgal, M. y Christopher, D. (2011). A Study on Selective Data Mining Algorithms. *IJCSI International Journal of Computer Science Issues, 8*(2), 479-483. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.402.7992&rep=rep1&type=pdf

Pérez Verona, I. y Arco García, L. (2016*)*. Una revisión sobre aprendizaje no supervisado de métricas de distancia. *Revista Cubana de Ciencias Informáticas, 10*(4), 43-67. https://www.researchgate.net/publication/317514053_Una_revision_sobre_aprendizaje_no_supervisado_de_metricas_de_distancia

Perichinsky, G., García-Martínez, R. y Proto, A. (2-7 de octubre de 2000). *Knowledge Discovery Based on Computational Taxonomy And Intelligent Data Mining* [Presentación en papel]. VI Congreso Argentino de Ciencias de la Computación, Ushuaia, Argentina.

Perversi, I. (2007). *Aplicación de minería de datos para la exploración y detección de patrones delictivos en Argentina*. [Tesis de Grado, Instituto Tecnológico de Buenos Aires]. Repositorio ITBA Principal.

Perversi I., Valenga F., Fernández F., Britos P. y García-Martínez, R. (3-4 de mayo de 2007). *Identificación y Detección de Patrones Delictivos basada en Minería de Datos*. IX Workshop de Investigadores en Ciencias de la Computación, Trelew, Argentina 2007.

Pezzuchi, G. (2012). Análisis criminal, confusiones varias y experiencias en la Provincia de Buenos Aires, Argentina. En P. Tudela Poblete (Ed.), *Buenas prácticas para el análisis delictual en América Latina*, (pp. 23-39). Fundación Paz Ciudadana. https://pazciudadana.cl/biblioteca/documentos/buenas-practicas-para-el-analisis-delictual-en-america-latina/

Piquero, A. y Weisburd, D. (2010). *Handbook of Quantitative Criminology*. Springer

Pitropakis, N., Panaousis, E., Giannetsos, T., Anastasiadis, E. y Loukas, G. (2019). A Taxonomy and Survey of Attacks against Machine Learning. *Computer Science Review, 34*. https://doi.org/10.1016/j.cosrev.2019.100199

Prabakaran, S. y Mitra, S. (5-6 de enero de 2018). *Survey of analysis of crime detection techniques using data mining and machine learning* [Presentación en papel]. Congreso Nacional de Técnicas Matemáticas y sus Aplicaciones, Kattankulathur, India.

Ramió, C. (2019). La gobernanza pública de la inteligencia artificial y de la robotización. En C. Ramió (Ed.), *Inteligencia Artificial y Administración Pública: Robots y humanos compartiendo el servicio público* (pp. 126-165). Los libros de la Catarata.

Refaeilzadeh, P., Tang, L. y Liu, H. (2009). Cross-Validation. En L. Liu y M.T. Özsu, (Eds.), *Encyclopedia of Database Systems*. Springer. https://doi.org/10.1007/978-0-387-39940-9_565

Resolución N° 1061 de 2002 [Ministerio de Justicia y Seguridad]. Por la cual se aprueba la puesta en funcionamiento de un sistema de recolección, procesamiento y análisis de la información delictiva. 2 de agosto de 2002.

Resolución N° 1062 de 2002 [Ministerio de Justicia y Seguridad]. Por la cual se aprueba la realización de cursos para el personal policial. 2 de agosto de 2002.

Reza, K., Javideh, M. y Reza, E. (2011). Detecting and investigating crime by means of data mining: a general crime matching framework. *Procedia Computer Science, 3*, 872-880. https://doi.org/10.1016/j.procs.2010.12.143

Rodríguez, P., Palomino, N. y Mondaca, J. (2017). *El uso de datos masivos y sus técnicas analíticas para el diseño e implementación de políticas públicas en Latinoamérica y el Caribe*. Banco Interamericano de Desarrollo. http://dx.doi.org/10.18235/0000694

Rummens, A., Hardyns, W. y Pauwels, L. (2017.) The use of predictive analysis in spatiotemporal crime forecasting: building and testing a model in an urban context. *Applied Geography, 86*, 255-261. https://doi.org/10.1016/j.apgeog.2017.06.011

Sáenz Vela, H. M. (2016). Revisando los métodos de agregación de unidades espaciales: MAUP, algoritmos y un breve ejemplo. *Estudios Demográficos y Urbanos*, *31*(2), 385–411. https://estudiosdemograficosyurbanos.colmex.mx/index.php/edu/article/view/1592

Salafranca Barreda, D. y Rodríguez Herrera, M. (julio de 2016). *Modelo SDIK: un sistema analítico para la predicción del delito* [Presentación en papel]. VII Conferencia Internacional sobre Análisis Delictual, Santiago de Chile, Chile.

Salvador, M. y Ramió, C. (2020). Capacidades analíticas y gobernanza de datos en la administración pública como paso previo a la introducción de la inteligencia artificial. *Revista del CLAD Reforma y Democracia*, (77), 5-36. https://clad.org/wp-content/uploads/2021/04/077-01-SR.pdf

Sayeh, W. y Bellier, A. (12-13 de diciembre de 2014). Neural Networks versus Logistic Regression: The Best Accuracy in Predicting Credit Rationing Decision [Presentación en papel]. Simposio Mundial de Banca Financiera 2014. Escuela de Negocios de Nanyang, Singapur.

Servente, M. (2002). *Algoritmos TDIDT aplicados a la minería de datos inteligente*. [Tesis de Grado, Universidad de Buenos Aires]. http://laboratorios.fi.uba.ar/lsi/servente-tesisingenieriainformatica.pdf

Shah, N., Bhagat, N. y Shah, M. (2021). Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention. *Visual Computing for Industry, Biomedicine, and Art, 4.* https://doi.org/10.1186/s42492-021-00075-z

Shojaee, S., Mustapha, A., Sidi, F. y Jabar, M. A. (2013). A study on classification learning algorithms to predict crime status. *International Journal of Digital Content Technology and its Applications, 7*(9), 361-369. https://doi.org/10.4156/jdcta.vol7.issue9.43

Silva Lira, I. (2000). *Costo económico de los delitos, niveles de vigilancia y políticas de seguridad ciudadana en las comunas del Gran Santiago*. CEPAL. https://repositorio.cepal.org/handle/11362/7258

Simon, A., Deo, M.S., Venkatesan, S. y Babu, D.R. (2016). An overview of machine learning and its applications. *International Journal of Electrical Sciences & Engineering*, 1(1), 22–24. https://www.researchgate.net/publication/289980169_An_Overview_of_Machine_Learning_and_its_Applications

Sozzo, M. (2008). Pintando a Través de Números: Fuentes Estadísticas de Conocimiento y Gobierno Democrático de la Cuestión Criminal en Argentina. En M. Sozzo (Ed.), *Inseguridad, prevención y policía* (Vol. 4, pp. 21-65). FLACSO. https://biblio.flacsoandes.edu.ec/libros/digital/46247.pdf

Sozzo, M. (2009). Gobierno local y prevención del delito en la Argentina. *URVIO, Revista Latinoamericana de Seguridad Ciudadana*, (6), 58-73. https://doi.org/10.17141/urvio.6.2009.1104

Stamp, M. (2017). *Introduction to machine learning with applications in information security*. Chapman and Hall/CRC. https://doi.org/10.1201/9781315213262

Tabedzki, C., Thirumalaiswamy, A. y van Vliet, P. (2018). *Yo home to Bel-Air: predicting crime on the streets of Philadelphia*. https://www.shivani-agarwal.net/Teaching/CIS-520/Spring-2018/Projects/40.pdf

Talaviya T., Shah D., Patel N., Yagnik H. y Shah M. (2020). Implementation of artificial intelligence in agriculture for optimisation of irrigation and application of pesticides and herbicides. *Artificial Intelligence in Agriculture*, *4*, 58–73. https://doi.org/10.1016/j.aiia.2020.04.002

Tallon, P. P. (2013). Corporate governance of big data: Perspectives on value, risk, and cost. *Computer*, *46*(6), 32-38. https://doi.org/10.1109/MC.2013.155

Tene, O. y Polonetsky, J. (2012). Privacy in the age of big data: A time for big decisions. *Stanford Law Review*, *64*, 63-69. https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/

Tyagi, D. y Sharma, S. (2018). An approach to crime data analysis: a systematic review. *International Journal of Engineering Technologies and Management Research*, *5*(2), 67-74. https://doi.org/10.29121/ijetmr.v5.i2.2018.615

Universidad de San Andrés (marzo 2021). *Encuesta de Satisfacción Política y Opinión Pública (ESPOP)*. https://udesa.edu.ar/sites/default/files/23-informe-espop-marzo-2021.pdf

Valdés Rabelo, S. (2020). *Detección de anomalías en serie de tiempo de datos del agua utilizando un enfoque de aprendizaje profundo*. [Tesis de Maestría, Universidad Autónoma de Chihuahua]. Repositorio digital - Universidad Autónoma de Chihuahua.

Valenga, F., Perversi, I., Fernández, E., Merlino, H., Rodríguez, D. Britos, P. y García-Martínez, R. (1-5 de octubre de 2007). *Aplicación de la minería de datos para la exploración y detección de patrones delictivos en Argentina* [Presentación en papel]. XIII Congreso Argentino de Ciencias de la Computación, Resistencia, Chaco, Argentina.

van Ooijen, C., Ubaldi, B. y Welby, B. (2019). *A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance*. OECD Working Papers on Public Governance, No. 33, OECD, https://doi.org/10.1787/09ab162c-en.

Vaquero Barnadas, M. (2016). *Machine learning applied to crime prediction*. [Tesis de Grado, Universidad Politécnica de Catalunya]. https://upcommons.upc.edu/bitstream/handle/2117/96580/MACHINE%20LEARNING%20APPLIED%20TO%20CRIME%20PREDICTION.pdf

Varshitha, D.N., Vidyashree, K.P., Aishwarya, P., Janya, T.S., Dhananjay Gupta, K.R y Sahana, R. (2017). Paper on Different Approaches for Crime Prediction system. *International Journal of Engineering Research & Technology*, *5*(20).

https://www.ijert.org/research/paper-on-different-approaches-for-crime-prediction-system-IJERTCONV5IS20013.pdf

Wahbeh, A.H., Al-Radaideh, Q.A., Al-Kabi, M.N. y Al-Shawakfa, E.M. (2011). A Comparison Study between Data Mining Tools over some Classification Methods. *International Journal of Advanced Computer Science and Applications, 2*(8), 59-66. https://www.researchgate.net/publication/251422102_A_Comparison_Study_between_DataMining_Tools_over_some_Classification_Methods/link/00b495345aa85dd423000000/download

Weisburd, D. y Britt, C. (2014). *Statistics in Criminal Justice.* (4ª ed.) Springer.

Wibowo, A.H. y Oesman, T.I. (2020). The comparative analysis on the accuracy of k-NN, naive Bayes, and decision tree algorithms in predicting crimes and criminal actions in Sleman regency. *Journal of Physics Conference Series, 1450*. https://doi.org/10.1088/1742-6596/1450/1/012076.

Zhang, H. y Wang, M. (2009). Search for the smallest random forest. *Statistics and Its Interface, 2*, 381–388. https://www.intlpress.com/site/pub/files/_fulltext/journals/sii/2009/0002/0003/SII-2009-0002-0003-a011.pdf