Estudios de Economía Aplicada
ISSN: 1133-3197
secretaria.tecnica@revista-eea.net
Asociación Internacional de Economía Aplicada
España

BADAL-VALERO, ELENA; GARCÍA-CÁRCELES, BELÉN
Detección de fraude financiero mediante redes neuronales de clasificación en un caso real español
Estudios de Economía Aplicada, vol. 34, núm. 3, 2016, pp. 693-709
Asociación Internacional de Economía Aplicada
Valladolid, España

Disponible en: http://www.redalyc.org/articulo.oa?id=30147485010

Cómo citar el artículo
Número completo
Más información del artículo
Página de la revista en redalyc.org

Sistema de Información Científica
Red de Revistas Científicas de América Latina, el Caribe, España y Portugal
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

ESTUDIOS DE ECONOMÍA APLICADA VOL. 34-3 2016 PÁGS. 693–710

Detección de fraude financiero mediante redes neuronales de clasificación en un caso real español *

ELENA BADAL-VALERO [a], BELÉN GARCÍA-CÁRCELES [a]

[a] *Universidad de Valencia, Facultad CC.EE., Avda. de los naranjos, s/n, 46022 Valencia, España. E-mail:* Elena.Badal@uv.es, Belen.Garcia-Carceles@uv.es

RESUMEN

Este análisis supone una primera aproximación a la implementación de modelos de redes neuronales al trabajo pericial para la detección de operaciones de fraude. Los datos analizados provienen de un caso real de blanqueo de capitales en el que se está colaborando con la Policía Nacional Española. En ellos se cuenta con información de operaciones contables individuales entre las que se cuenta con una proporción de operaciones bien identificadas como fraudulentas con la que es posible entrenar un modelo de clasificación. En este trabajo, tras describir brevemente la metodología utilizada y la estrategia de ajuste se obtiene un modelo con una capacidad predictiva reseñable, incluso con datos de entrenamiento fuertemente desequilibrados. Además, al aplicar técnicas de balanceado de los datos de entrenamiento (SMOTE) se obtiene un resultado que indicaría la viabilidad de este tipo de modelos como herramienta en la planificación y priorización de las tareas de investigación policial, ya que uno de los principales problemas de los investigadores expertos en estos delitos financieros es la incapacidad para traducir la gran cantidad de información que se deriva de las empresas implicadas en patrones de compra de los individuos claramente fraudulentos.

Palabras clave: Redes Neuronales, data mining, fraude financiero, blanqueo de capitales.

Detecting Financial Fraud using Neural Network Classification Models in a Real Spanish Case

ABSTRACT

This paper explores the possibilities offered by statistical tools based on artificial neural networks for pattern recognition in expert work for money-laundering detection. The data is provided by the Spanish Police Department and comes from a case in which is actually working at. Account information is provided, where some accounting entries are identified as fraud. Hence it is possible to use this information to train a classification model. In this analysis, after briefly describing methodology used and fitting strategy, it is presented a model with a promising predictive capacity, even with strongly unbalanced training data set. After applying balancing technique to the training data (SMOTE) the result is remarkably improved which would indicate the viability of those models as tool for police experts planification, providing a way to reduce the use of expensive research resources.

Keywords: Artificial Neural Network, Data Mining, Financial Fraud, Money Laundering, Forensic Accounting.

Clasificación JEL: C450, D220, L51

* *Las autoras agradecen el apoyo del Ministerio de Economía y Competitividad a través del proyecto CSO2013-43054-R. Elena Badal-Valero agradece al programa Vali+d de la Generalitat Valenciana, Conselleria d´Educació, Investigació, Cultura i Esport. Belén García-Cárceles agradece la financiación del programa Atracció al Talent del Vicerrectorado de Investigación de la Universitat de València.*

Artículo recibido en mayo de 2016 y aceptado en septiembre de 2016
Artículo disponible en versión electrónica en la página www.revista-eea.net, ref. ə-34309

ISSN 1697-5731 (online) – ISSN 1133-3197 (print)

1. INTRODUCCIÓN

El blanqueo de capitales es un delito económico que ha evolucionado en el tiempo y que se ejecuta a distintos niveles y en diversas magnitudes. Las cuantías defraudadas oscilan desde el tradicional blanqueo de pequeñas cantidades de dinero proveniente del tráfico minorista y local de drogas, hasta las grandes cantidades (miles de millones de euros) de macro estructuras empresariales que han surgido en las últimas décadas y que operan a escala internacional (Khac y Kechadi, 2010).

A este problema se suma el hecho de que los actuales avances tecnológicos, así como los sistemas de comunicación, han puesto a disposición de los solventes delincuentes herramientas con las que crear estructuras grandes, complejas y coordinadas de empresas con las que evitar la detección del fraude económico (ingeniería financiera) (Petrucelli, 2012).

Por ello, el reto que afrontan los cuerpos de seguridad especializados en esta área es doble: por una parte deben ser capaces de identificar las grandes redes de blanqueo, y por otra, conseguir seleccionar, de la cantidad de información que se deriva de las empresas implicadas, aquella que permita identificar claramente los patrones de compra de los individuos que ocultan blanqueo. Sin embargo, con las técnicas tradicionales se hace muy complicado cumplir estos objetivos (Dutta, 2013).

La aplicación de herramientas estadísticas basadas en redes neuronales artificiales para la detección de patrones de comportamiento han sido aplicadas con buenos resultados en campos tan heterogéneos como el mercado inmobiliario (Caridad y Ceular, 2001), el área biomédica (Uberbacher y Mural, 1991) o en mercados financieros (Muñiz y Alvarez, 1997) (Olmedo y Velasco, 2007), por lo que en este estudio se explora las posibilidades que ofrecen estas herramientas estadísticas para el reconocimiento de patrones de fraude en operaciones individuales.

La base de datos corresponde a datos contables de una empresa matriz investigada por la Policía Nacional Española que contiene información proveniente de los registros efectuados en el transcurso de una investigación por delitos de blanqueo de capitales. Concretamente, contiene más de doce millones de datos extraídos de la contabilidad interna de la empresa núcleo de una estructura empresarial potencialmente defraudadora.

La autoridad policial desarrolla un papel fundamental en el proceso de análisis ya que son los responsables de detectar, investigar y extraer la información que se procesa en este estudio y, es de acuerdo a sus conclusiones que se consiguen identificar las operaciones que son fraudulentas. Dado que los recursos de los investigadores son limitados, en la mayoría de casos no es realista esperar que sea posible hacer un seguimiento exhaustivo de todas las empresas de la

organización y por tanto se centran en las que consideran más delictivas[1]. Es por este motivo que la red se entrena con un número limitado de operaciones fraudulentas detectadas lo que permite el ajuste de un modelo de clasificación mediante la combinación de las características de las operaciones, de modo que al introducir nuevas puedan ser clasificadas como potencialmente fraudulentas.

Por el procedimiento de análisis aquí descrito se persigue ofrecer a los investigadores una forma objetiva de identificar, de entre las operaciones pendientes de investigar, aquellas que pudieran ser fraudulentas, ayudando a priorizar los recursos de investigación disponibles hacia las empresas que concentran mayor potencial de fraude.

El artículo se organiza como sigue: En el apartado segundo se presentan los conceptos de fraude demostrado y sospecha de fraude y se especifica el modelo de red neuronal artificial que va a utilizarse en todo el análisis. El tercer apartado recoge la estrategia de ajuste, su justificación y limitaciones. Es también en este apartado donde se explora la sensibilidad del modelo al conjunto de entrenamiento y las posibilidades de mejora al balancearlo utilizando SMOTE. El último apartado recoge brevemente las conclusiones y las posibilidades de investigación que se abren a la luz de los resultados obtenidos.

2. DESCRIPCIÓN DE LA METODOLOGÍA

Es de esperar que el modelo de Redes Neuronales sea tan bueno como el "ojo policial" y que aporte una forma de detectar un mayor número de operaciones de fraude. Por tanto, el objetivo del modelo ajustado es identificar correctamente el mayor número de operaciones fraudulentas posible, siendo importante minimizar la proporción de operaciones fraudulentas mal clasificadas (falsos positivos).

Las variables disponibles en la base de datos que caracterizan una operación:

1. El artículo: variable discreta que recoge los 42 tipos de artículos que se comercializaron.
2. El almacén de la mercancía: variable discreta que indica el lugar donde se realizó la compra de producto al proveedor, 12 localizaciones.
3. El/la Administrativo/a: persona que gestiona la operación en el departamento de administración. 43 administrativos/as.
4. El importe total pagado al proveedor por la adquisición del producto. Variable continua.

[1] En el caso objeto de estudio se tiene constancia de que la red de empresas la formaban más de 500 empresas entre proveedores y mayoristas.

5. El margen bruto de beneficio de la operación, importe total ingresado por la venta del material al cliente menos el importe total pagado al proveedor. Variable continua.
6. La cantidad de material contenida en el artículo. Variable continua.
7. Margen de descuento aplicado en la operación. Variable continua.

No se tiene conocimiento a priori de qué artículos, personas o lugares están envueltos en la trama de blanqueo de capitales, sólo se tiene acceso a la identificación de un pequeño número de operaciones fraudulentas (18,99% del total) que la policía ha podido demostrar como tal a través de sus procedimientos de investigación.

Es de reseñar que estos procedimientos se basan en la vigilancia de las personas involucradas en la trama, siendo posterior la detección de dichas operaciones a través de los movimientos contables. Por tanto, aquellas operaciones que no se han detectado como fraudulentas no dejan de ser sospechosas. Es por esto que conviene concretar las siguientes definiciones:

1. Fraude demostrado: consideraremos como fraude demostrado aquellas operaciones que hayan podido ser verificadas por la policía como tal.
2. Fraude sospechoso: el resto de operaciones.

2.1. El fraude demostrado

En primer lugar, se analizan las características mencionadas en las operaciones de fraude demostrado. Con estas descripciones no se pretende hacer juicios de valor "a priori" sobre qué variables deben tenerse en cuenta a la hora de identificar un fraude potencial en el modelo de red. Precisamente, una de las ventajas de este tipo de modelo es que pueden incorporar toda la información disponible en su estructura.

En la Tabla 1 se recoge el recuento de operaciones según artículo. Se muestra únicamente los 18 códigos de artículo más frecuentes, que representan el 94,27% de las operaciones. Se ordena según el número de operaciones de fraude demostrado.

Tabla 1
Variable "Código de Artículo"

Código Artículo	Operaciones "Fraude Demostrado"	Número de Operaciones	% "Fraude Demostrado"
ART1	16.950	139.877	12,12
ART2	10.258	38.240	26,83
ART3	2.665	6.066	43,93
ART4	2.220	6.714	33,07
ART5	2.070	4.880	42,42

Tabla 1 ***(Continuación)***
Variable "Código de Artículo"

Código Artículo	Operaciones "Fraude Demostrado"	Número de Operaciones	% "Fraude Demostrado"
ART6	1.286	2.349	54,75
ART7	1.071	23.462	4,56
ART8	876	2.755	31,80
ART9	597	4.307	13,86
ART10	586	2.248	26,07
ART11	476	6.526	7,29
ART12	467	1.081	43,20
ART13	392	10.227	3,83
ART14	368	3.473	10,60
ART15	364	1.970	18,48
ART16	348	1.686	20,64
ART17	314	1.009	31,12
ART18	297	834	35,61

Fuente: Elaboración propia.

Por su parte, la Tabla 2 muestra el recuento de operaciones para todos los almacenes en los que se realizan las operaciones y la Tabla 3 los 20 administrativos que más operaciones gestionan, representando el 91,18% de las operaciones totales.

Tabla 2
Variable "Almacén"

Consigna	Operaciones "Fraude Demostrado"	Número de Operaciones	% "Fraude Demostrado"
ALM1	40.369	217.985	18,52
ALM2	1.284	6.936	18,51
ALM3	929	9.619	9,66
ALM4	912	21.966	4,15
ALM5	230	1.036	22,20
ALM6	79	79	100,00
ALM7	55	181	30,39
ALM8	0	15.241	0
ALM9	0	881	0
ALM10	0	334	0

Fuente: Elaboración propia.

Tabla 3
Variable "Administrativos"

Administrativo	Operaciones "Fraude Demostrado"	Número de Operaciones	% "Fraude Demostrado"
PEX1	9.829	39.191	25,08
PEX2	7.246	20.494	35,36

Tabla 3 ***(Continuación)***
Variable "Administrativos"

Administrativo	Operaciones "Fraude Demostrado"	Número de Operaciones	% "Fraude Demostrado"
PEX3	6.255	37.412	16,72
PEX4	3.903	14.308	27,28
PEX5	2.605	4.609	56,52
PEX6	2.042	12.501	16,33
PEX7	2.005	8.414	23,83
PEX8	1.917	24.947	7,68
PEX9	1.872	9.386	19,94
PEX10	925	4.530	20,42
PEX11	904	4.497	20,10
PEX12	804	2.565	31,35
PEX13	648	1.817	35,66
PEX14	620	10.768	5,76
PEX15	448	1.694	26,45
PEX16	429	12.538	3,42
PEX17	330	698	47,28
PEX18	282	1.463	19,28
PEX19	206	38.239	0,54

Fuente: Elaboración propia.

Finalmente, en la Tabla 4 se recogen los descriptivos de las variables continuas disponibles, en concreto, se dispone del importe total de cada operación, la cantidad de material que contiene cada compra y los márgenes de descuento y de beneficio.

Tabla 4
Variables continuas: importe total, cantidad de material, margen de descuento y margen bruto de beneficio

	Mín.	P25	Mediana	Media	P75	Máx.	NA´s
Importe total							
Fraude	-0,18	1,03	4,10	36,62	37,11	2.799,15	733,86
Resto	-0,18	1,74	12,91	68,81	68,00	1.818,30	153,30
Cantidad de Material							
Fraude	0	13	78	201	260	18.560	6.517
Resto	0	51	166	277	377	9.980	2.211
Margen de descuento							
Fraude	0	0	1,00	1,00	1,00	1,02	230
Resto	0	0	1,00	0,95	1,00	1,80	79
Margen Bruto de Beneficio							
Fraude	-25,53	0,01	0,03	0,66	0,04	40,60	5.612
Resto	-17,39	0,01	0,03	0,36	0,04	28,64	663

Fuente: Elaboración propia.

Al realizar este sencillo ejercicio descriptivo los datos parecen determinar ciertos patrones de fraude (artículos y administrativos con mayor proporción de implicación en las operaciones de fraude, mayor margen bruto de beneficio …) sin embargo, la ingeniería financiera a la que pueden acceder estas empresas hace desconfiar de la fiabilidad de estas apariencias.

De hecho, la realidad muestra que dichos patrones no son tan determinantes como a priori pudiera parecer para que, finalmente, se pueda demostrar que una operación (y, sobre todo las personas implicadas en ellas) estén delinquiendo. De ahí que se busque una alternativa en la que pueda incorporarse la mayor cantidad de información disponible que, en modelos más sencillos e interpretables, no sea posible captar la complejidad de las relaciones que lleven a una adecuada detección de operaciones de fraude en base a sus características.

2.2. Especificación del modelo de red

Este análisis supone una primera aproximación a la implementación de modelos de redes neuronales al trabajo pericial para la detección de operaciones de fraude. Por ello se ha utilizado una estructura de red muy sencilla: la red de propagación hacia atrás (del inglés "Back-Propagation network") o perceptron de una capa oculta (del inglés "Single Hidden Layer Perceptron").

En esta estructura de red hay tres elementos: las unidades de salida de la red (outputs, *Y*), las unidades de entrada (inputs, *X*) y las características derivadas de los inputs (*Z*) (Hastie *et al.*, 2008).

Las unidades ocultas, Z, se obtienen como una combinación lineal de los inputs, transformada mediante una función de activación que se define como la función sigmoidea:

$$\sigma(\upsilon) = 1/(1+e^{-\upsilon})$$

donde: $\sigma(\upsilon) = [0,1]$, y $\upsilon =]-\infty, +\infty[$

Para una clasificación en k clases, hay *K* unidades en la salida de la red, con la k-ésima unidad modelizando la probabilidad para la clase *k*. Hablamos, por tanto de *k* medidas objetivo Y_k, $k = 1,\ldots, K$, codificadas como 0,1. La estructura de la red se representa mediante las tres expresiones siguientes:

$$Z_m = \sigma(\alpha_{0m} + \alpha_m^T X), \qquad m = 1,...,M,$$

$$T_K = \beta_{0k} + \beta_k^T Z, \qquad k = 1,...,K,$$

$$f_k(X) = g_k(T) \qquad k = 1,...,K,$$

donde: $Z = (Z_1, Z_2, ..., Z_M)$, y $T = (T_1, T_2, ..., T_k)$.

Los parámetros del modelo (pesos o ponderaciones), inicialmente desconocidos, se ajustan utilizando los errores Deviance (en el caso de redes de clasifi-

cación), definidos como:

$$R(\theta) = -\sum_{i=1}^{N} \sum_{k=i}^{K} y_{ik} \log fk(k_i)$$

Además, pueden incorporarse unidades de sesgo tanto en los nodos intermedios como en la función de salida que, pensadas como un input adicional, capturarían los interceptos α_{0m} y β_{0k}. El conjunto completo de pesos Θ se denota como:

$$\{\alpha_{0m}, \alpha_m; m = 1, 2, ..., M\}\, M(p+1)\, pesos,$$

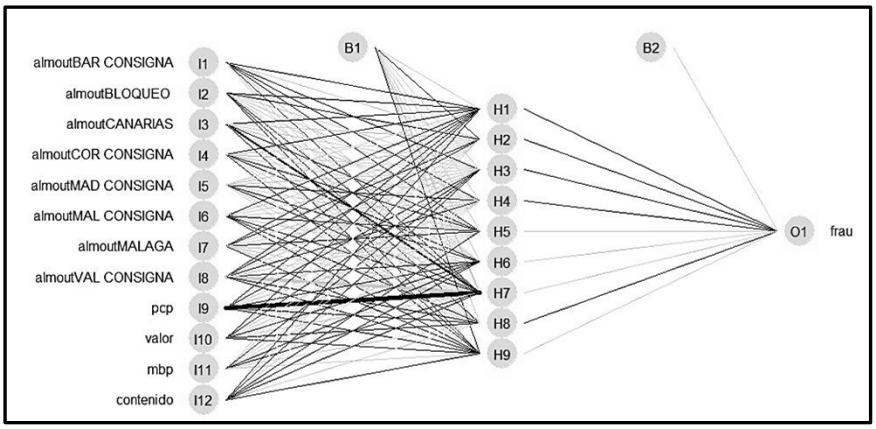
$$\{\beta_{0k}, \beta_k; m = 1, 2, ..., M\}\, K(M+1)\, pesos,$$

Finalmente, la función de salida $g_k(T)$, permite la transformación final de los vectores de salida T, utilizando la función de transformación softmax (en el caso concreto) definida como:

$$g_k(T) = \frac{e^{T_k}}{\sum_{l=1}^{K} e^{T_L}}$$

Por tanto, el modelo de red neuronal es un modelo no lineal multilogit que utiliza una transformación de los inputs (X), mediante pesos (Θ) fijados a través de la minimización de los errores (Deviance, $R(\Theta)$) mediante un procedimiento de actualización back-propagation (Ripley, 1996).

Figura 1
Esquema de la estructura de red ajustada.



Nota: Sólo se representan las variables input I1 a I12 para mayor claridad. Si bien la estructura de la red en el caso de estudio considera 101 inputs.

Fuente: Elaboración propia.

En el caso concreto que se analiza en este trabajo, la estructura de la red se ha recogido en la Figura 1 (Beck, 2015). En ella existe una único nodo en la

salida (Y_k=1) codificada 0 (no es posible concluir que la operación es fraudulenta) y 1 (la operación es identificada como fraudulenta), representada en el extremo derecho de la figura con O1.

Las llamadas características derivadas (Z_m, m = 1,..,9) son los nodos H1 a H9, que se crean a partir de combinaciones lineales de las variables consideradas (inputs: I1 a I100, X_p, p = 1,...,100). En la estructura representada en la Figura 1 puede también apreciarse la inclusión de variables que pretenden capturar el sesgo en cada uno de los nueve nodos de la capa oculta (el vector de pesos B1, α_{0m}) y en la función de salida (el peso B2, β_{0k}).

3. IDONEIDAD DE LA ESTRUCTURA DE RED "BACK PROPAGATION NETWORK" PARA LA DETECCIÓN DEL FRAUDE DEMOSTRADO

3.1. Estrategia de muestreo para el conjunto de entrenamiento

El proceso de ajuste se inicia testando las limitaciones de los recursos informáticos disponibles. Es decir, teniendo en cuenta la magnitud de la base de datos disponible y la estructura de red que se desea aplicar es necesario establecer una estrategia para encontrar un compromiso entre estructura de la red y cantidad de datos a incluir en el conjunto de entrenamiento, que no comprometa la finalidad del análisis.

La estrategia seguida es la siguiente:

1. El set de entrenamiento será tal que el desequilibrio en los datos sea comparable a la muestra de operaciones de la policía, en el que la proporción de operaciones fraudulentas respecto al resto se sitúa en torno al 19%. Es decir, siendo Am el número operaciones fraude de la muestra, Bm el número de resto de operaciones, Ace el número operaciones fraude del conjunto de entrenamiento y Bce el número de resto de operaciones del conjunto de entrenamiento, se cumple que:

$$\frac{Am}{Bm} \approx \frac{Ace}{Bce} \approx 19\%$$

2. Si bien lo habitual es reservar el 20% de los datos para el conjunto comprobación y utilizar el 80% en el de entrenamiento, en este caso la proporción será la opuesta (80% comprobación, 20% entrenamiento) ya que se prioriza el número de nodos de la capa oculta de la red y la utilización de todas las variables disponibles.

Esta decisión se fundamenta en tres motivos: por una parte se desea maximizar el aprovechamiento de la estructura; por otra, si no se tomaran todas las variables de entrada se estarían tomando decisiones "a priori" en relación a la inclusión/exclusión de variables, lo que iría en contra de los objetivos estable-

cidos en este trabajo; finalmente, utilizar menos datos asegura que los resultados obtenidos, en cualquier caso, tiendan a estar por debajo de los que cabría esperar con mayor información (estrategia conservadora adecuada al enfoque de "primera aproximación" que se desea aportar con este trabajo).

Así, el ajuste se realiza manteniendo todos los inputs de entrada de la red (101), 9 nodos en la capa oculta de la red y un número de operaciones de entrenamiento por debajo del habitual (50.000 operaciones, el 20% del total de operaciones disponibles).

3. Además, siguiendo una estrategia conservadora, en este apartado se presentan los resultados del modelo de red especificado sin aplicar corrección alguna, es decir, el ajuste se realiza sin utilizar técnicas que permitieran compensar alguno de los problemas que habitualmente se señalan en relación a este tipo de datos (remuestreo (Buhlmann y Yu, 2002), ensamblado (Meir y Rätsch, 2003), técnicas de sobremuestreo o inframuestreo (SMOTE-Boost de Chawla *et al.*, 2003)).

La finalidad de esa estrategia es obtener un resultado a partir del cual se puedan aplicar mejoras sucesivas (el balanceado de los datos se aborda en el apartado siguiente) y esperar un mayor ajuste del modelo conforme pudieran superarse las limitaciones informáticas.

3.2. Punto de partida: modelo ajustado con datos desequilibrados

Utilizando el entorno de programación de R (R Core Team, 2015) se ha empleado el paquete de R nnet (Venables y Ripley, 2002) de la librería del mismo nombre, ajustando sus parámetros conforme a las especificaciones descritas y se evalúa el ajuste del modelo mediante el enfoque tradicional: construyendo una matriz de confusión (Tabla 5), donde se confrontan las operaciones bien y mal clasificadas basadas en el conjunto de comprobación. En ella se especifican los recuentos utilizados para el cálculo de las tasas con las que evaluar los resultados (Tabla 6) mediante la tasa de operaciones bien clasificadas (*TBC*), la de operaciones fraudulentas bien clasificadas (verdaderos positivos, *sensitivity* o *recall*, *TVP*) y c) operaciones fraudulentas mal clasificadas (falsos positivos, TFP).

Formalmente sería: $TBC = \frac{\left(P_{11} + P_{22}\right)}{\left(P_{11} + P_{12} + P_{21} + P_{22}\right)} 100; TVP = \frac{\left(P_{22}\right)}{\left(P_{21} + P_{22}\right)} 100; TFP = \frac{\left(P_{21}\right)}{\left(P_{21} + P_{22}\right)} 100$

La tasa de ajuste global del modelo es reseñable, con un 72,16% de operaciones bien clasificadas. Esta tasa desciende al 17,63% cuando se trata de operaciones de fraude bien clasificadas. Por su parte, la tasa de falsos positivos es elevada (superior al 80%) aunque hay que interpretarla con cuidado, ya que incluye en su recuento operaciones fraudulentas no detectadas por la policía pero que en realidad lo son. Es decir, como se ha explicado al inicio del punto 2,

las operaciones que no han sido detectadas como fraude no dejan de ser "sospechosas".

Tabla 5
Matriz de confusión

		Clasificación según el modelo	
		Resto (0)	**Fraude (1)**
Clasificación Policial	Resto (0)	P_{11}	P_{12}
	Fraude (1)	P_{21}	P_{22}

Fuente: Elaboración propia.

Tabla 6
Tasas obtenidas a partir de la matriz de confusión

Operaciones Bien Clasificadas	72,16%
Operaciones Mal Clasificadas	27,83%
TVP (*recall)*	17,63%
TFP	82,36%

Nota: TVP = Tasa de Verdaderos Positivos, operaciones fraudulentas bien clasificadas; TFP = Tasa de falsos positivos, operaciones fraudulentas mal clasificadas; Operaciones bien clasificadas (TBC).

Fuente: Elaboración propia.

La tasa de ajuste global del modelo es reseñable, con un 72,16% de operaciones bien clasificadas. Esta tasa desciende al 17,63% cuando se trata de operaciones de fraude bien clasificadas. Por su parte, la tasa de falsos positivos es elevada (superior al 80%) aunque hay que interpretarla con cuidado, ya que incluye en su recuento operaciones fraudulentas no detectadas por la policía pero que en realidad lo son. Es decir, como se ha explicado al inicio del punto 2, las operaciones que no han sido detectadas como fraude no dejan de ser "sospechosas".

Teniendo en cuenta que no se han utilizado técnicas para compensar el desequilibrio inicial de la base de datos, ni para considerar el coste de los errores de clasificación, el resultado es, por lo menos, prometedor.

3.3. Posibilidades de mejora: Sensibilidad a cambios en el conjunto de entrenamiento

En este apartado se realiza un experimento para evaluar la sensibilidad del modelo a cambios en el conjunto de entrenamiento con dos objetivos. En primer lugar, dado que se ha seguido una estrategia de muestreo por la que se limita la cantidad de información en el entrenamiento de la red al 20% de los datos disponibles (ver apartado 3.1) es conveniente obtener una medida de la influencia de esta decisión en el ajuste. Esta medida, además, es una magnitud de las posi-

bilidades de mejora del ajuste que no se limita sólo a superar las restricciones de potencia de cálculo informático, sino que puede afrontarse aplicando técnicas de balanceado de los datos mediante remuestreo (tal como se aborda en el apartado siguiente). En segundo lugar, es un hecho conocido que los pesos que el modelo asigna a los nodos de la red son altamente sensibles a cambios en el conjunto de datos de entrenamiento debido al procedimiento de actualización de gradiente descendente del diseño *back-propagation*.

La estrategia seguida es la siguiente: se establecen 100 conjuntos de entrenamiento del mismo tamaño que el anterior (50.000 operaciones diferentes cada uno) y con el mismo ratio Ace/Bce (19%). Se ajustan 100 modelos de red con la misma estructura anterior, fijando los mismos pesos iniciales y utilizando todo el conjunto de inputs disponibles (nuevamente, se emplea la función del paquete de R nnet (*op. cit.*)). Para cada modelo se han obtenido los ratios antes definidos a partir de las correspondientes matrices de confusión y sus conjuntos de comprobación.

La Tabla 7 recoge el valor promedio y la desviación típica del ajuste para los 100 modelos. La variabilidad alrededor de la media (11,2% para los verdaderos positivos y 88,98% para los falsos positivos) se sitúa por debajo de los 4 puntos porcentuales.

Tabla 7
Ajuste de los 100 modelos de red

	Media	Desviación Típica	Coeficiente de asimetría
Operaciones Bien Clasificadas	76,50%	2,5113%	1,549
Operaciones Mal Clasificadas	23,50%		
TMVP	11,02%	3,697%	1,547
TMFP	88,98%		

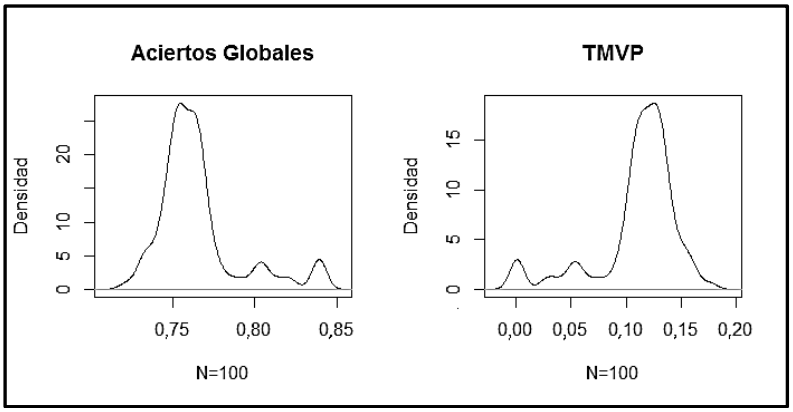
TMVP = Tasa Media de Operaciones Fraudulentas bien clasificadas.
TMFP= Tasa Media de Operaciones Fraudulentas mal clasificadas.

$$TMVP = \sum_{i=1}^{100} \frac{\left(P_{22}^{i}\right)}{\left(P_{21}^{i} + P_{22}^{i}\right)}; TMFP = \sum_{i=1}^{100} \frac{\left(P_{21}^{i}\right)}{\left(P_{21}^{i} + P_{22}^{i}\right)} .$$

Fuente: Elaboración propia.

En el experimento realizado para detectar la sensibilidad del ajuste a cambios en el conjunto de entrenamiento, se observa que la distribución de verdaderos positivos es asimétrica (Figura 2) debido a un grupo de 14 modelos cuya proporción cae por debajo del 7,5% sin los que se obtiene que la tasa de verdaderos positivos $TVP \sim N(12,3\%,1,7\%)$. La asimetría indicaría que la exclusión/inclusión de casos en el conjunto de entrenamiento no es neutral: la estrategia de selección aleatoria deja margen para la mejora.

Figura 2
Distribución de densidad de las tasas calculadas en los 100 modelos



Fuente: elaboración propia.

3.4. Ajuste mediante balanceado del conjunto de entrenamiento

En el caso que nos ocupa cabe destacar que: a) no se dispone de información acerca del coste asociado a clasificar erróneamente una operación fraudulenta lo que limita el uso de medidas sensibles al coste (matriz de costes, curvas de coste), b) la proporción de operaciones fraudulentas en la muestra es muy inferior respecto del resto de operaciones y c) la estrategia de selección del conjunto de entrenamiento no es neutral.

Las técnicas de muestreo permiten compensar la falta de información de la clase minoritaria (operaciones fraudulentas) en el conjunto de entrenamiento a la vez que implican una forma alternativa para considerar en el proceso de aprendizaje los costes asociados a los errores de clasificación. Una combinación de sobremuestreo de la clase minoritaria e inframuestreo de la mayoritaria puede ser la estrategia con mejores resultados (Japkowicz, 2000). Ahora bien, si se aplica de forma aleatoria, el inframuestreo puede llevar a eliminar ejemplos importantes de la información de entrenamiento, cuestión que, como se ha visto en el apartado anterior, puede llevar a un rendimiento muy pobre del clasificador. Por su parte, el sobremuestreo aleatorio de la clase minoritaria puede llevar al sobreajuste y a la falta de generalidad, ya que crea regiones de decisión más pequeñas y específicas.

Una alternativa es generar sintéticamente nuevos ejemplos que amplíen la información para aquellos casos de la clase minoritaria difíciles de clasificar. SMOTE (de *Synthetic Minority Oversampling Technique*) es una técnica que proporciona información nueva relativa a la clase minoritaria además de infrarrepresentar la clase mayoritaria (Chawla *et al*., 2002). Con esta técnica se generan ejemplos sintéticos en el segmento que une un ejemplo de la clase minorita-

ria con sus *k* vecinos más próximos, dependiendo de la cantidad de ejemplos sintéticos que se requieran, se escogerán aleatoriamente vecinos de estos *k* vecinos. Para cada clase se considera el voto de los vecinos más próximos con lo que la región de decisión es más grande y menos específica (hay más puntos, está mejor descrita), a diferencia de las regiones más pequeñas y específicas que se crean con el muestreo aleatorio.

Al aplicar la técnica de SMOTE[2] al mismo modelo del apartado 3.2, a partir de su matriz de confusión (Tabla 8) se obtienen los resultados recogidos en la Tabla 9.

Tabla 8
Matriz de confusión al aplicar SMOTE

		Clasificación según el modelo	
		Resto (0)	**Fraude (1)**
Clasificación Policial	Resto (0)	41,72%	42,33%
	Fraude (1)	4,88%	11,05%

Fuente: Elaboración propia.

Tabla 9
Tasas obtenidas a partir de la matriz de confusión al aplicar SMOTE

Operaciones Bien Clasificadas	52,77%
Operaciones Mal Clasificadas	47,22%
TVP (*recall)*	69,36%
TFP	30,63%

Nota: TVP = Tasa de Verdaderos Positivos, operaciones fraudulentas bien clasificadas; TFP = Tasa de falsos positivos, operaciones fraudulentas mal clasificadas; Operaciones bien clasificadas (TBC).

Fuente: Elaboración propia.

La mejora obtenida es reseñable por varios motivos. En primer lugar destaca el descenso de la tasa de falsos positivos de 82,36% del modelo con un conjunto de entrenamiento desequilibrado (Tabla 6) a 30,63%. En segundo lugar, la proporción de operaciones fraudulentas bien clasificadas asciende del 17,66% del modelo inicial al 69,36% en el modelo con SMOTE.

La importancia de esta mejora no es baladí, dado que la diferencia de utilizar el modelo del apartado 3.2 como soporte a las tareas periciales frente al modelo con SMOTE, implica reducir considerablemente la probabilidad de malgastar recursos policiales en investigar empresas y personas detrás de operaciones que el modelo indica como fraudulentas y que en realidad no lo son.

[2] Se utiliza la función *SMOTE* del paquete de R DMwR (Torgo, L. 2010).

En la Tabla 8 se observa también un claro descenso de las Operaciones Bien Clasificadas de forma global (52,77%) en este nuevo modelo en relación a los resultados de la Tabla 6 (72,16%). Sin embargo, tal como se discute en los párrafos anteriores lo relevante es acertar bien las operaciones fraudulentas, dado que las operaciones no fraudulentas en realidad pudieran serlo.

Por tanto, el uso de estos modelos en la detección de casos reales de fraude financiero, junto con la implementación de técnicas de muestreo como SMOTE que mejoren el desequilibrio de los datos, puede servir de herramienta a los investigadores para conocer patrones de comportamiento en casos de blanqueo de capitales y ofrecer mayor información para su detección, así como también orientar a las autoridades a aquellas empresas cuyos comportamientos aparentan ser fraudulentos.

4. CONCLUSIONES

Los resultados obtenidos en la exploración de los modelos de red como herramienta de trabajo en la actividad pericial han sido notables. Por un lado, ha sido posible incorporar toda la información (variables) disponibles en la estimación del modelo. Por otro lado, la rapidez con la que se ha obtenido el ajuste ha sido destacable.

En el modelo ajustado con datos de entrenamiento sin balancear se observa que la tasa de ajuste es reseñable, con un 72,16% de operaciones bien clasificadas. Esta tasa desciende al 17,63% cuando se trata de operaciones de fraude bien clasificadas. Por su parte, la tasa de falsos positivos (superior al 80%) hay que interpretarla con cuidado, ya que incluye en su recuento operaciones fraudulentas no detectadas por la policía pero que en realidad lo son.

La estrategia de muestreo seguida para la selección del conjunto de datos de entrenamiento no es neutral, tal como se constata con el experimento realizado con 100 conjuntos de entrenamiento distintos para detectar la sensibilidad del ajuste a cambios en el conjunto de entrenamiento. Se observa que la distribución de verdaderos positivos es asimétrica debido a un grupo de 14 modelos cuya proporción cae por debajo del 7,5% sin los que se obtiene que la tasa de verdaderos positivos $TVP \sim N(12{,}3\%, 1{,}7\%)$. La asimetría indicaría que la exclusión/inclusión de casos en el conjunto de entrenamiento no es neutral: la estrategia de selección aleatoria deja margen para la mejora.

Del experimento anterior y de la propia metodología de ajuste propia de la estructura de red utilizada, así como el desconocimiento de los costes asociados a los errores de clasificación llevan a aplicar una estrategia de mejora con datos de entrenamiento balanceados utilizando la técnica SMOTE. Se observa cómo, a pesar de descender la tasa de aciertos globales, la capacidad de detección de

operaciones fraudulentas mejora hasta alcanzar casi un 70%, que prácticamente alcanza la tasa de aciertos globales del modelo sin balancear.

Así, habiéndose conseguido un ajuste reseñable se han detectado importantes oportunidades de mejora a través de la revisión de la estrategia de selección de casos para el conjunto de entrenamiento, como por ejemplo, la exploración de otras estructuras de red y otros métodos de aprendizaje. Además, también se podría combinar el modelo con diferentes estrategias de balanceado como la de tipo "*Boosting*" (Freund y Schapire, 1996) que junto con la técnica SMOTE (SMOTE Boost de Chawala *et al.*, 2003) permitiría mejorar la identificación de las operaciones fraudulentas.

Finalmente, los resultados aquí obtenidos abren un amplio abanico de posibilidades a la mejora del trabajo pericial en la detección del fraude financiero y el blanqueo de capitales utilizando este tipo de herramientas predictivas para lo que sería deseable, mediante el uso de análisis de sensibilidad, la búsqueda de patrones de fraude que puedan describirse "a priori".

REFERENCIAS BIBLIOGRÁFICAS

BECK, M.W. (2015). *"NeuralNetTools: Visualization and Analysis Tools for Neural Networks".* Version 1.4.0. Disponible en: http://cran.r-project.org/web/packages/NeuralNetTools/ [27/07/2016].

BÜCHLMANN, P., YU B. (2002). "Analyzing Bagging". The Annals of Statistics. Vol. 30, No. 4, pp. 927-961.

CHAWLA, N. V., BOWYER, K. W., HALL, L. O., y KEGELMEYER, W. P. (2002). "*Smote: Synthetic minority over-sampling technique*". Journal of Artificial Intelligence Research, pp. 321-357.

CARIDAD, J. M., & CEULAR, N. (2001). "*Un análisis del mercado de la vivienda a través de redes neuronales artificiales"*. Estudios de economía aplicada, (18), pp. 67-81.

CHAWLA, N. V., LAZAREVIC, A., HALL, L. O., and BOWYER, K. W. (2003b). *"Smoteboost: Improving Prediction of the Minority Class in Boosting"*. In Seventh European Conference on Principles and Practice of Knowledge Discovery in Databases, Vol.16, pp. 107-1 19, Dubrovnik, Croatia.

DUNCAN, L.T., and CRAN TEAM.(2016). Package 'RCurl'. Disponible en: https://cran.r-project.org/web/packages/RCurl/index.html [27/07/2016].

DUTTA, S. (2013). *Statistical Techniques for Forensic Accounting*. Upper Saddle River (NJ): FT Press.

GOH, A.T. (1995). "Back-propagation neural networks for modelling complex systems". *Artificial Intelligence in Engineering*, Vol.9, nº3, pp. 143-151.

HASTIE, T., TIBSHIRANI, R., y FRIEDMAN, J. (2008). *The Elements of Statistical Learning. Data Mining, Inference, and Prediction* (2nd ed.). Standfor: Springer. (pp. 392-396).

HEIDARINIA, N., HAROUNABADI, A., y SADEGHZADEH, M. (2014). *"An intelligent Anti-Money Laundering Method for Detecting Risky Users in the Banking Systems"*. International Journal of Computer Applications. No.22, pp. 35-39.

JAPKOWICZ, N. (2000), *"The Class Imbalance Problem: Significance and Strategies".* In Proceedings of the 2000 International Conference on Artificial Intelligence (IC-AI'2000): Special Track on Inductive Learning, Las Vegas, Nevada.

KHAC, N. L., y KECHADI, M. (2010). *"Application of Data Mining for Anti-Money Laundering Detection: A Case Study"*. IEEE International Conference on Data Mining Workshops.

LIN-TAO, JI, N., y ZHANG, J.-L. (2008). *"A RBF neural network model for anty-money laundering"*. International Conference on Wavalet Analysis and Pattern Recognition, pp. 209-215.

MEIR, R., y RÄSTCH, G. (2003). "*An introduction to boosting and leveraging*". Lecture Notes in Computer Science, pp 118-183.

MUÑIZ, P. y J. A. ÁLVAREZ (1997). "*Comportamiento del Mercado: Hipótesis alternativas*". Revista de Bolsas y Mercados Españoles, Vol.60, pp 29-33.

NGAI, E., HU, Y., WONG, Y.,CHEN, Y., y SUN, X. (2011). *"The application of data mining techniques in financial fraud detection: A classification frame work and an academic review of literature"*. Decision Support Systems, Vol.50, nº3, pp. 559-569.

OLDEN, D. (2005). "*Illuminating the "black box": a randomization approach for understanding variable contributions in artificial neural networks".* Ecological Modelling, nº 154, pp. 135-150.

OLMEDO, E., VELASCO, F., & VALDERAS, J. M. (2007). "*Caracterización no lineal y predicción no paramétrica en el IBEX35*". Estudios de Economía Aplicada, 25(3).

PETRUCELLI, J. (2012). *Detecting Fraud in Organizations: Techniques, Tools, and Resources*. Washington DC: John Wiley & Sons, Inc.

R CORE TEAM (2015). R: A language and environment for statistical computing. R Foundation for Statistical Computing,Vienna, Austria, ISBN 3-900051-07-0, URL http://www.R-project.org/

RIPLEY. (1996). *Pattern Recognition and Neural Networks*. Cambridge University:Press.

SHMIELD, R. y AMES, M. (2013). *"Next generation detection engine for fraud and compliance"*. SAS Global Forum, pp. 1-6.

TORGO, L. (2010) *Data Mining using R: learning with case studies*, CRC Press (ISBN: 9781439810187).

UBERBACHER, E. C., & MURAL, R. J. (1991). "*Locating protein-coding regions in human DNA sequences by a multiple sensor-neural network approach*". Proceedings of the National Academy of Sciences, 88(24), pp.11261-11265.

U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT. (1995). *"Information Technologies for Control of Money Laundering"*. Washington, DC: U.S: U.S. Government Printing Office. pp. 55-72.

VENABLES , W.N. y RIPLEY, B. (2002). *Modern Applied Statistics with S*. 4th Edition. New York: Springer.

WICKHAM, H. (2015). stringr: Simple, Consistent Wrappers for Common String Operations. R package version 1.1.0. https://CRAN.R-project.org/package=stringr

WICKHAM, H, y CHANG, W. (2016). devtools: Tools to Make Developing R Packages Easier. R package version 1.12.0. https://CRAN.R-project.org/package=devtools.