

Gestión del fraude en la industria energética



Diseño y Maquetación

Dpto. Marketing y Comunicación
Management Solutions - España

Fotografías

Archivo fotográfico de Management Solutions
iStock

© Management Solutions 2017

Todos los derechos reservados. Queda prohibida la reproducción, distribución, comunicación pública, transformación, total o parcial, gratuita u onerosa, por cualquier medio o procedimiento, sin la autorización previa y por escrito de Management Solutions.

La información contenida en esta publicación es únicamente a título informativo. Management Solutions no se hace responsable del uso que de esta información puedan hacer terceras personas. Nadie puede hacer uso de este material salvo autorización expresa por parte de Management Solutions.

Índice



Introducción

4



Resumen ejecutivo

8



Gestión del fraude

12



Técnicas de gestión del fraude en el sector energético

22



Ejemplo de aplicación de técnicas de modelización: hurto de energía

30



Conclusiones

36



Bibliografía

38



Glosario

40

Introducción



El fraude se ha convertido en una de las principales preocupaciones de los gobiernos y compañías; de hecho, se estima que las pérdidas por fraude en las organizaciones pueden oscilar entre el 5% y el 9% de sus beneficios anuales¹. Para tener un mayor entendimiento de los diferentes marcos de gestión del fraude, es necesario conocer en qué consiste, sus componentes y las distintas formas en las que puede presentarse.

En el mundo empresarial, el fraude se asocia a una acción contraria a la verdad y rectitud, que perjudica a la organización contra la que se comete. El fraude puede comprometer a una empresa, ya sea externamente por los clientes, proveedores y otras partes o internamente por empleados, directivos o propietarios.

El **contexto actual** presenta entre otras las siguientes características y oportunidades:

- ▶ Disponibilidad creciente de datos **sobre clientes, empleados, proveedores**, etc., su interacción con la compañía y sus hábitos de comportamiento.
- ▶ Avance en las **técnicas de análisis y cuantificación de la propensión o probabilidad** de ocurrencia de eventos de fraude.

- ▶ Desarrollo de **metodologías y sistemas para combatir el fraude interno** mediante la **segregación de funciones (SoD, segregation of duties)**.

La **aportación de valor** de estos mecanismos de gestión se refleja tanto en su vertiente económica (según un estudio de la ACFE², las pérdidas por fraude a nivel mundial se redujeron un 54% gracias a la adopción de medidas de monitorización proactiva de datos³), como reputacional y de cumplimiento. Estos últimos aspectos son especialmente relevantes dado el entorno regulatorio actual que fomenta la inversión y la implantación de medios para la gestión del fraude.

¹ Mark Button, Jim Gee, Graham Brooks, "Measuring the cost of fraud: an opportunity for the new competitive advantage", Journal of Financial Crime, Vol. 19.

² Association of Certified Fraud Examiners (ACFE): Report to the nations on occupational fraud and abuse. 2016 Global Fraud Study: "proactive data monitoring was associated with 54% lower losses and frauds detected in half the time". Análisis de un total de 2.410 casos de fraude ocupacional de todo el mundo para el año 2016 (48% en EEUU).

³ A través de, entre otros, análisis de datos, supervisión de los directivos/managers, establecimiento de un contacto para recibir denuncias, auditorías sorpresa, etc.



El objetivo de este documento es compartir ciertas reflexiones **sobre el concepto de fraude**, así como sobre los principales elementos empleados para su gestión y las oportunidades de optimización que afloran con los avances tecnológicos, como por ejemplo las tecnologías de *Big Data* y *Analytics* entre otras. Éstas están basadas en la disponibilidad y análisis de grandes volúmenes de información y la aplicación de metodologías de **perfilación y segmentación**.

Particularizando en la industria energética, en este documento se describen eventos concretos de **fraude en el sector energético** que, por su representatividad y consumo de recursos en las compañías, requieren de un tratamiento específico y donde las técnicas de detección y su integración en la gestión adquieren mayor relevancia.

- ▶ Con relación al fraude externo, las compañías energéticas que distribuyen electricidad y/o gas natural están expuestas al hurto de energía mediante conexiones o accesos fraudulentos a la red. La gestión de este tipo de fraude se apoya en métodos para cuantificar la probabilidad de que una medición no refleje el suministro real. Los métodos empleados son variados (como regresiones logísticas, redes neuronales, árboles de decisión, etc.), están aplicados en esquemas de *machine learning* y están orientados a discriminar suministros "razonables" de suministros potencialmente fraudulentos. Estas técnicas se apoyan en el uso de variables que caracterizan el cliente, su perfil de consumo, hábitos de comportamiento, etc. con el

objetivo de identificar perfiles o comportamientos anómalos o propensos al hurto de energía (p.ej. reincidentes). No es objeto de este documento el tratamiento de los ciberataques, si bien estos suponen amenazas de suplantación de identidad o intervención de las comunicaciones, generando por ejemplo, interrupciones de suministro.

- ▶ Por lo que respecta al fraude interno, la principal preocupación se centra en las pérdidas asociadas a eventos de fraude en procesos críticos para la compañía, como puede ser el ciclo comercial de una comercializadora energética. Estos sucesos se ubican principalmente en los procesos de facturación y cobro, en los cuales la posibilidad de alterar consumos, importes, procesos de compra o datos bancarios puede permitir sustraer ingresos a la compañía. La gestión de este tipo de fraude se realiza mediante metodologías orientadas a la segregación de funciones, el control de accesos a los sistemas comerciales y económico-financieros y la definición de indicadores y esquemas de reporting de la existencia de violaciones a la segregación de funciones.

Adicionalmente el presente documento mostrará cómo los métodos de modelización, perfilación y segmentación se complementan con la implantación de una metodología de **cuantificación de la utilidad económica de las actuaciones** que discrimina la calidad de la segmentación realizada para la detección del fraude (o efecto de los modelos de segmentación) frente a la bondad de la



ejecución de las actuaciones (o efecto de las propias campañas de detección), con el objetivo de **evaluar la rentabilidad por separado de la inversión en técnicas de modelización de la inversión en inspecciones de detección de hurto**. En este sentido, la inversión en gestión del fraude se evalúa como una inversión más de la compañía.

Estas técnicas están soportadas en **plataformas de modelización** que combinan componentes de tratamiento masivo de datos con *software* estadístico y **herramientas de control de accesos** y gestión de roles, incompatibilidades, etc.

Finalmente, se incluyen en esta publicación unos **ejemplos de aplicación** de técnicas de modelización de la probabilidad de detectar hurto de energía (un caso particular de fraude externo). Estos modelos se apoyan en la caracterización del punto de suministro mediante variables que identifican los factores subyacentes al fraude, tales como las características físicas del medidor o contador, información comercial y sociodemográfica del cliente o usuario, histórico de consumo y comportamiento en relación al hurto, otras operaciones con el cliente, vinculación, reclamaciones o resultado de inspecciones, etc.

Se demuestra por tanto la **aportación de valor del dato**, de la información de clientes y operaciones (consumos horarios, datos de clientes, accesos a sistemas, etc.), en la cuantificación de las posibilidades de ocurrencia de eventos de fraude y su uso para la optimización de actuaciones tanto

preventivas (p. ej. segregación de funciones o control de accesos a sistemas) como mitigantes (p. ej. ejecución de campañas de inspección y la segmentación de perfiles según su propensión al hurto). Así, la estimación de probabilidades de ocurrencia de un evento de hurto o la posibilidad de realizar actuaciones fraudulentas en el ciclo comercial, combinadas con la materialidad de los potenciales impactos (energía defraudada, importes sustraídos, etc.) permiten realizar una **priorización de las actuaciones bajo un racional económico y de rentabilidad**.

De hecho, según los datos ofrecidos por una de las principales compañías europeas de distribución de electricidad, tras el uso de los datos disponibles con los medidores inteligentes, el porcentaje de casos de fraude detectados que afectaban a dicha compañía pasó de un 5% a un 50%⁴.

⁴Fragkioudaki, A. et al. (2016). Detection of Non-technical Losses in Smart Distribution Networks: A Review.



Resumen ejecutivo



Consideraciones de contexto

1. Si bien no existe una definición única, a los efectos del presente documento calificaremos como **fraude** cualquier acción u omisión intencionada diseñada para engañar a otros, resultando en una pérdida para estos, y/o en una ganancia para el defraudador⁵.
2. Las prácticas fraudulentas más comunes pueden agruparse en dos dominios: **fraude externo** (por ejemplo hurto, suplantación, ciberataques, etc.) y **fraude interno** (fraude contable, fiscal, operación en beneficio propio, etc.⁶).
3. Existen tres **factores**, que de darse de forma simultánea implicarán un incremento de la probabilidad de que una persona cometa un fraude:
 - Necesidad o presión, bien de índole económica o de otra naturaleza. Debe existir un incentivo o una necesidad (interna) o presiones (externas), que inciten o motiven a que el individuo cometa la acción de fraude.
 - Oportunidad percibida. Para que un fraude tenga lugar debe existir una debilidad a explotar en un determinado proceso. El sujeto percibe una manera de resolver sus problemas de forma fraudulenta con una baja asunción del riesgo de ser descubierto.
 - Racionalización/Actitud. Justificación del acto delictivo. En este sentido influyen los valores morales del sujeto, la percepción que el sujeto tiene de los valores éticos que rigen la empresa (víctima del fraude), así como la valoración del beneficio que supone el fraude frente a las posibles consecuencias negativas que puede acarrear en caso de ser descubierto.
4. Al analizar los **eventos** de fraude reportados por cada industria, destaca el porcentaje de incidentes asociados al sector bancario/financiero, que sigue siendo la industria que presenta mayor número de casos. No obstante, al analizar las pérdidas medias asociadas a cada caso por industria, el sector de la minería y el comercio al por mayor son los que presentan mayores pérdidas medias, situándose el sector bancario en una situación intermedia (con respecto a las industrias analizadas en un estudio de la ACFE⁷).
5. En el caso de la **industria energética**, si bien tiene una incidencia menor según ese mismo estudio (aproximadamente un 5% de los casos analizados se concentran en utilities y corporaciones de *oil&gas*), presenta algunas particularidades asociadas al hurto de energía en las que técnicas de modelización pueden aportar un valor diferencial.
6. El proceso de **transformación digital** en el que están inmersos todos los sectores implica una mayor exposición al riesgo de fraude, ya que los avances tecnológicos son aprovechados por los autores de fraude para adoptar nuevas estrategias, no recogidas en los planes históricos de prevención, detección y actuación de las compañías.
7. Debido al **carácter cambiante de las prácticas fraudulentas**, su detección es un proceso continuo y dinámico que requiere por parte de las organizaciones tener definido un marco de actuación que incluya estrategias, enfoques y políticas concretas y específicas, y en el que todas las áreas involucradas actúen de forma coordinada. En este contexto, las compañías han ido armando una política (o políticas) para la gestión del fraude que, atendiendo al origen del evento fraudulento, establece responsabilidades de gestión y control.
8. Por todo ello, cobra especial interés la implantación de un **marco de gestión del fraude**, cuya complejidad puede variar desde iniciativas sencillas de despliegue de controles tácticos (procesos de autorización y validación, alarmas, inspecciones, etc.) hasta la ejecución de proyectos globales que, dando alcance a la mayoría de los procesos de la compañía, persiguen establecer métricas de medición del riesgo de fraude en los mismos y modificar los propios procesos y los sistemas para su mitigación (implantación de plataformas de segregación de funciones, control de accesos, modelización de la propensión al fraude, sistemas informacionales y esquemas de reporting para su medición, etc.).
9. Las **funciones** de gestión del fraude en una compañía se encuentran habitualmente **dispersas**, siendo

⁵ The Institute of Internal Auditors (IIA), The American Institute of Certified Public Accountants (AICPA) y Association of Certified Fraud Examiners (ACFE) (2012): Managing the Business Risk of Fraud: A Practical Guide.

⁶ De acuerdo con el marco de Basilea II (BCBS: Convergencia internacional de medidas y normas de capital), de aplicación en el sector financiero (si bien esta definición es de aplicabilidad general).

⁷ Association of Certified Fraud Examiners (ACFE): Report to the nations on occupational fraud and abuse. 2016 Global Fraud Study.



generalmente cada área de negocio afectada la responsable y promotora de iniciativas para su gestión, apoyada por las áreas de tecnología que le dan servicio. No obstante, en parte debido al desarrollo de funciones de cumplimiento dentro de las compañías (como el CCO o *Chief Compliance Officer*) y a la búsqueda de la eficiencia económica y la optimización de procesos, existe una tendencia a la centralización de metodologías, indicadores y mecanismos de control del fraude.

10. La gestión del fraude se ha visto reforzada por **sistemas inteligentes** y de **análisis estadístico** para su detección. Estas técnicas, que permiten detectar las nuevas estrategias y patrones empleados por los infractores, combinan elementos puros de análisis y modelización como *data mining* y *machine learning*, elementos técnicos de computación de alto rendimiento como stream computing y, finalmente, procesos completos de transformación de datos para la adquisición de conocimiento útil como *knowledge discovery in database* (KDD).

Técnicas de gestión del fraude aplicadas en el sector energético

11. El aumento en la capacidad de generar, almacenar y procesar **información** puede ser aprovechado para tener acceso en tiempo real a la caracterización de un cliente, una operación, un proceso, etc., identificando así comportamientos indicativos de propensión al hurto de energía. El empleo de la ciencia del dato (*Data Science*) para la detección del fraude en el sector energético resulta de gran utilidad por ejemplo para diferenciar el porcentaje de energía perdida en la red de distribución asociado a pérdidas técnicas (no representativas de un

evento de fraude) y pérdidas no técnicas (hurto de energía y por tanto representativas de un evento de fraude). Con todo ello, la inversión en modelos de detección avanzados optimiza las tasas de éxito de las campañas de inspección y mejora la detección del fraude. En todo caso, para avanzar con garantías en la implantación de este tipo de modelos conviene previamente definir e implementar un marco de referencia que facilite el gobierno de los datos, modelos y procesos asociados.

12. Los **modelos** a desarrollar pretenden encontrar patrones, tendencias o reglas que expliquen el comportamiento del cliente antes de la detección del fraude. Las técnicas a emplear variarán en función del fin perseguido y del tipo de dato utilizado. El aprovechamiento de todo el potencial que representan las técnicas de *Data Science* incorpora dos elementos clave:

- El análisis en tiempo real. Los sistemas de recopilación de información permiten llevar a cabo la captura y el seguimiento de los datos en tiempo real. Además, es posible programar algoritmos que hagan uso de dicha información, lo cual facilita y agiliza la detección de los nuevos patrones y estrategias de fraude no empleadas hasta ese momento por los infractores.
- El reentrenamiento automático y autoaprendizaje. Los modelos de detección del fraude son recalibrados de forma automática (con escasa intervención de los analistas) e iterativamente a partir de los grandes volúmenes de datos, lo cual se traduce en una potencial mejora del poder predictivo durante los sucesivos reentrenamientos.



Ejemplo de modelización aplicado al hurto de energía

13. Uno de los usos más extendidos del *Data Science* en la gestión del fraude en el sector energético consiste en maximizar la eficiencia de las **campañas de inspección**. La detección del fraude energético, asociado al consumo ilegal de energía en la red, parte de una segmentación de los clientes basada en su **probabilidad de cometer fraude**. Las técnicas de modelización aplicadas en la gestión de la detección de fraude energético permiten mejorar la tasa de éxito en la selección de clientes a ser inspeccionados.
14. Algunas **variables** que se han demostrado de alto poder predictivo son: datos del medidor, datos sociodemográficos, datos de consumo histórico de energía, datos de la operación o gestión realizada, mantenimiento de la red y de los medidores, información de cortes e irregularidades o información de contactos o reclamaciones con el cliente, etc.
15. Con el fin de identificar los **modelos** que mejor explican el comportamiento de los clientes fraudulentos se fijan algunos criterios mínimos que deben cumplir los resultados obtenidos por el modelo seleccionado, tales como su capacidad discriminante. Adicionalmente a la validación estadística, se validan los modelos con las inspecciones realizadas durante seis meses y se observa que, sea cual sea el número de inspecciones, las técnicas de *machine learning* son las que permiten generar segmentos con una mayor concentración de hurtadores.
16. Las áreas de gestión de la pérdida no técnica de las compañías energéticas invierten recursos humanos, técnicos y económicos en la ejecución de inspecciones a clientes. La **rentabilidad** de estas inversiones viene determinada por:
- las tasas de éxito observadas (del subconjunto de los clientes inspeccionados, qué porcentaje de clientes con hurto de energía se identificó);
 - la ganancia de energía (representada como valor económico de recuperación por cliente);
 - el número de clientes inspeccionados de la población objetivo;
 - y el coste unitario asociado a la inspección del cliente y por tanto el coste total de la campaña.
17. Se ha realizado un **ejercicio cuantitativo** aplicando la metodología expuesta, y se ha seleccionado un algoritmo específico por su mayor poder discriminante. Con este modelo se desarrolla un ejemplo de aplicación práctica en la configuración de campañas de inspección. En el ejemplo se multiplica por 3 la tasa de éxito de las inspecciones, llegando a un 27% (más de una de cada cuatro inspecciones son exitosas).

Gestión del fraude



Contexto

Concepto de fraude

No existe una definición unificada y homogénea de las prácticas que se consideran fraude. De hecho, una de las preocupaciones de los organismos internacionales es precisamente definir un marco legal unificado, en el que se establezcan criterios comunes sobre las prácticas que deben ser consideradas como fraudulentas, así como las sanciones a aplicar en cada caso.

No obstante, de acuerdo con la ACFE⁸ se define fraude como **“cualquier acción u omisión intencionada diseñada para engañar a otros, resultando en una pérdida para estos, y/o en una ganancia para el defraudador”**⁹. El fraude en el contexto empresarial se asocia a una acción contraria a la verdad y rectitud, que perjudica a la organización contra la que se comete. El fraude puede comprometer a una empresa, ya sea originado externamente en los clientes, proveedores y otras partes, o internamente en empleados, directivos, funcionarios o propietarios de la empresa.

Por tanto, las distintas prácticas fraudulentas más comunes pueden agruparse en estos dos dominios: fraude externo (por ejemplo hurto, suplantación, ciberataques, etc.) y fraude interno (fraude contable, fiscal, operación en beneficio propio, etc.). Es habitual considerar tanto el fraude externo como interno como dos categorías de riesgo operacional que las compañías identifican, miden y gestionan.

Se considera **fraude externo** al evento que hace sufrir una pérdida inesperada de tipo financiera, material o reputacional debido a actos fraudulentos llevados a cabo por una persona externa a la empresa. Se define como *“pérdidas derivadas de actuaciones por parte de un tercero encaminadas a defraudar, apropiarse de bienes indebidamente o a soslayar la legislación”*¹⁰.

Este puede llevarse a cabo por clientes, o bien por competidores o terceros:

- ▶ Clientes que utilizan bienes o servicios de forma fraudulenta, sin pagar por ello, falsifican medios de pago, manipulan procesos de compras, etc.
- ▶ Competidores, proveedores, terceros en general, que manipulan licitaciones, facturan a la empresa por bienes o servicios no prestados, ofrecen sobornos a empleados, etc.

En esta segunda categoría, las organizaciones se enfrentan en particular a amenazas de violaciones de la seguridad y robos de la propiedad intelectual cometidos por terceros desconocidos (p.ej. a través de ciberataques). Otros ejemplos de fraudes son la piratería, el robo de información confidencial, el fraude fiscal, la quiebra fraudulenta, el fraude asociado a seguros, el fraude asociado a la atención médica, etc.

El **fraude interno** es el originado en el interior de una organización y es cometido por sus empleados en contra de dicha organización/empleador. Se define como *“pérdidas derivadas de actuaciones encaminadas a defraudar, apropiarse de bienes indebidamente o a soslayar regulaciones, leyes o políticas empresariales en las que se encuentra implicada, al menos, una parte interna de la empresa en beneficio propio”*¹¹. Suele estar originado por un conflicto existente entre los intereses personales de un empleado o grupo de empleados y los de la organización. Se estima que en promedio una organización pierde el 5% de sus beneficios anuales solamente como resultado del fraude originado internamente¹².

Factores subyacentes al fraude

A la hora de gestionar el riesgo de fraude, las compañías deben identificar y monitorizar los distintos factores que pueden motivar un evento de fraude. Una de las herramientas empleadas para la evaluación del riesgo de fraude es el conocido como *“triángulo del fraude”*¹³ (véase fig.1). Esta herramienta constituye un modelo ampliamente aceptado a la hora de explicar los factores subyacentes que motivan a una persona a cometer fraude.

Según esta teoría, existen tres factores, que de darse de forma simultánea implicarán un incremento de la probabilidad de que una persona cometa un fraude:

- ▶ **Necesidad o presión.** Motiva el delito en primer lugar. Representa la presión a la que se ve sometido el sujeto debido a la existencia de un problema que no es capaz de

⁸ Association of Certified Fraud Examiners, organización dedicada a la formación en la prevención de fraude a nivel internacional.

⁹ Fuente: “Gestión del Riesgo de Fraude en las Organizaciones: Una Guía Práctica.” IIA, Institute of Internal Auditors.

¹⁰ Según la definición de Basilea: BCBS: Convergencia internacional de medidas y normas de capital. Junio 2004.

¹¹ Según la definición de Basilea II.

¹² Report to the nations on occupational fraud and abuse. 2016 Global Fraud Study. ACFE, Association of Certified Fraud Examiners.

¹³ Concepto desarrollado por el Dr. Donald R. Cressey, sociólogo y criminólogo, cuya investigación se centró en malversadores a los que llamó “violadores de confianza” (Other People’s Money, Montclair: Patterson Smith, 1973).

Fig. 1. Triángulo del fraude



resolver por medios legítimos, lo que le lleva a considerar actos ilegales como medio para solucionar dicho problema. Estas presiones pueden ser de índole económica o de otra naturaleza. Debe existir un incentivo o una necesidad (interna) o presiones (externas), que inciten o motiven a que el individuo cometa la acción de fraude.

- ▶ **Oportunidad percibida.** Define el método por el cual se cometerá el delito. Para que un fraude tenga lugar debe existir una debilidad a explotar en un determinado proceso (p.ej. ausencia de controles, poca segregación de funciones o ausencia de un marco de gestión del fraude correcto y actualizado). El sujeto percibe una manera de resolver sus problemas de forma fraudulenta con una baja asunción del riesgo de ser descubierto.
- ▶ **Racionalización/Actitud.** Justifica y valida el acto delictivo; es decir, se refiere a la habilidad del individuo para racionalizar y justificar internamente los actos incorrectos que suponen el acto fraudulento. En este sentido influyen los valores morales del sujeto, la percepción que tiene de los valores éticos que rigen la empresa (víctima del fraude), así como la valoración del beneficio que supone el fraude frente a las posibles consecuencias negativas que puede acarrear en caso de ser descubierto. La posición individual ante el riesgo y la honestidad son aspectos fundamentales y determinantes.

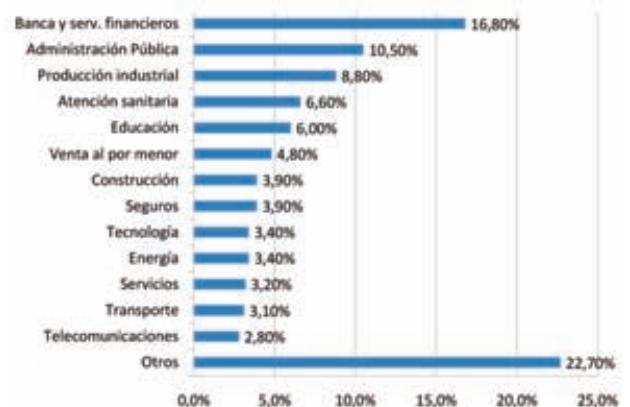
El valor del *triángulo del fraude* identifica los factores objetivos que tienen que estar presentes para que tenga lugar un evento de fraude. El reconocimiento de estos factores objetivos ayuda en la definición de las acciones a tomar para prevenir, detectar y dar respuesta al fraude.

Fraude por sectores de actividad

Los casos de fraude son un problema común en todas las industrias, lo que refuerza la necesidad de establecer controles y mecanismos que minimicen la existencia de dichos acontecimientos.

Al analizar los eventos de fraude reportados por cada industria, destaca el porcentaje de incidentes asociados al sector bancario/financiero, que sigue siendo la industria que presenta mayor número de casos (véase fig. 2).

Al analizar las pérdidas medias asociadas a cada caso por industria, el sector de la minería y el comercio al por mayor son los que presentan mayores pérdidas medias, situándose el sector bancario en una situación intermedia (con respecto a las industrias analizadas en el estudio de la ACFE). El sector energético, si bien tiene una incidencia menor según ese mismo estudio (aproximadamente un 3,4% de los casos analizados se concentran en *utilities* y corporaciones de *oil&gas*), presenta algunas particularidades asociadas al hurto de energía en las que técnicas de modelización pueden aportar un valor diferencial.

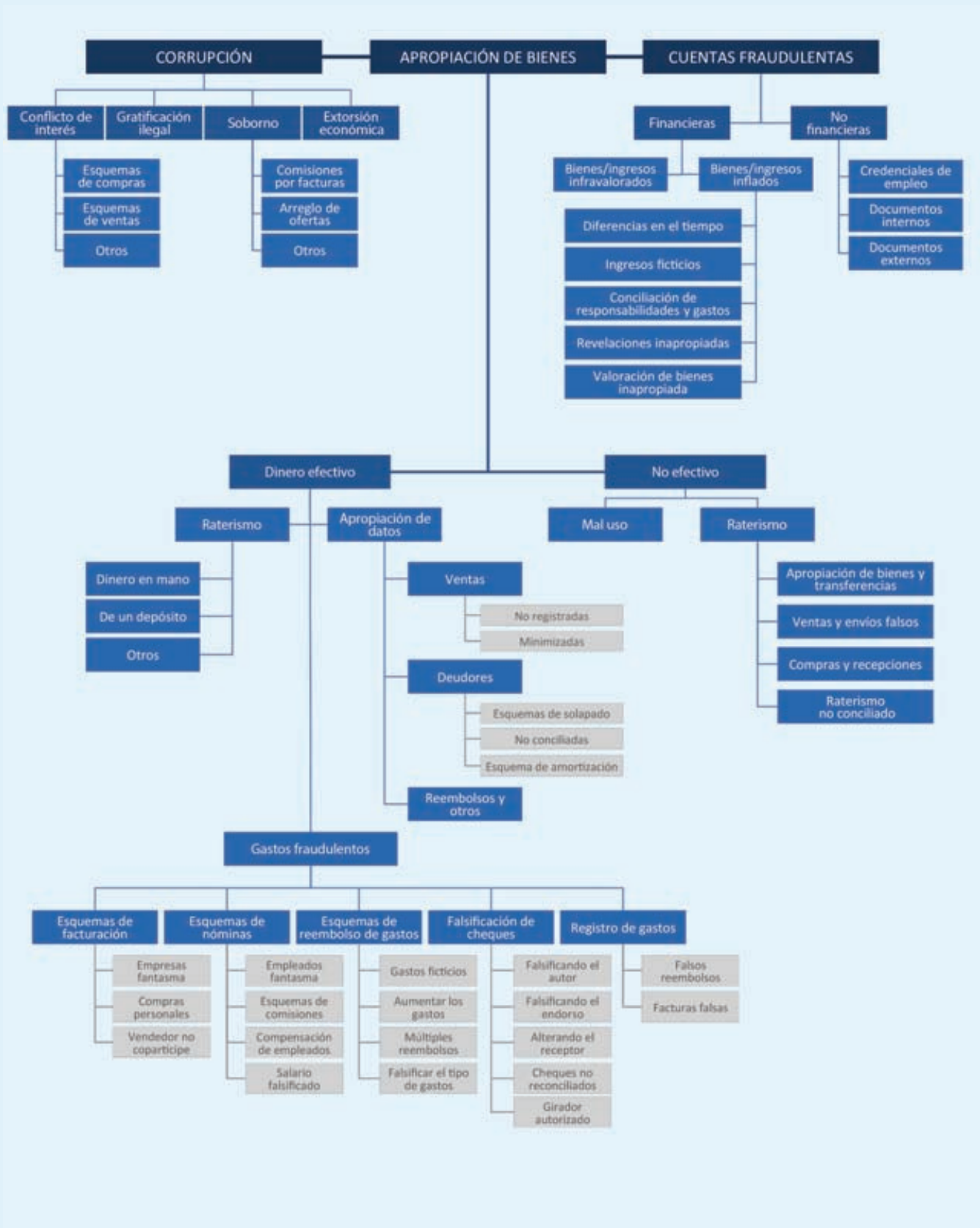
Fig. 2. Distribución en % de casos de fraude por sectores de actividad¹⁴

Fuente: 2016 Global Fraud Study: Report to the nations on occupational fraud and abuse (ACFE)

¹⁴ Otros: Servicios profesionales y sociales, Agricultura y Pesca, Real Estate, Utilities, Arte y Entretenimiento, Comercio al por mayor, Minería y Comunicaciones.

Sistema de clasificación del fraude y abuso profesional

Este tipo de fraude laboral puede ser clasificado según el siguiente “árbol” o esquema del fraude¹⁵:



¹⁵ Association of Certified Fraud Examiners (ACFE): Report to the nations on occupational fraud and abuse. 2016 Global Fraud Study.

Un elemento común a todos los sectores es el **proceso de transformación digital** en el que están inmersos. Ello implica una mayor exposición al riesgo de fraude, ya que los avances tecnológicos son aprovechados por los autores de fraude para adoptar nuevas estrategias, no recogidas en los planes históricos de prevención, detección y actuación de las compañías.

Aparece así el concepto de **ciberseguridad**, definida como la capacidad para proteger o defender el uso del ciberespacio de los ataques cibernéticos¹⁶. En los últimos años se ha agravado el riesgo asociado a la ciberseguridad derivado principalmente de tres factores: i) el desarrollo tecnológico, ii) los procesos de reestructuración de la industria y iii) la profesionalización de los atacantes.

No obstante, la digitalización de las distintas industrias es también una ventaja para las organizaciones a la hora de luchar contra el fraude, sobre todo en lo referente a su prevención y detección. El acceso a **grandes volúmenes de información**, así como el desarrollo de nuevas técnicas y modelos que permiten el **análisis del comportamiento de los clientes** (mediante técnicas de segmentación avanzadas p.ej. *machine learning*) constituyen herramientas efectivas para combatir el fraude y son aplicables en las distintas industrias¹⁷.

Estas soluciones están diseñadas para analizar automáticamente las distintas operaciones que se registren en los sistemas de las compañías. Deben ser capaces de procesar los grandes volúmenes de datos disponibles para detectar en tiempo real los distintos patrones y estrategias diseñadas por el defraudador. Estas técnicas mejoran los mecanismos actuales de prevención y detección de las actividades fraudulentas, ya que son capaces de detectar de forma dinámica patrones y estrategias fraudulentas no empleados anteriormente.

Debido al **carácter cambiante de las prácticas fraudulentas**, su detección es un **proceso continuo y dinámico**, lo que requiere por parte de las organizaciones tener definido un marco de actuación que incluya estrategias, enfoques y políticas concretas y específicas, y en el que todas las áreas involucradas actúen de forma coordinada. No obstante, el tratamiento del fraude presenta en ocasiones debilidades como consecuencia de la existencia de enfoques parciales y habitualmente dispersos; procesos en parte externalizados y no integrados en la gestión diaria del negocio; falta de coordinación entre las áreas responsables de la prevención, detección y respuesta ante los eventos de fraude (equipo anti-fraude, auditoría interna, seguridad de la red, seguridad de sistemas, etc.); diferenciación no siempre clara entre Primera Línea de Defensa (Gestión) y Segunda Línea de Defensa (Control), etc.

A continuación se introducen algunos ejemplos de tipos de fraude comunes en los sectores bancario, asegurador, de las telecomunicaciones y energético.

Sector bancario/financiero

Según se mostraba en la figura anterior, este puede ser uno de los sectores más afectados por el fraude en cuanto a número de ocurrencias. Además, los eventos de fraude en el sector afectan a todos los productos ofrecidos por los bancos (tarjetas de crédito y débito, cuentas corrientes, cheques, préstamos, etc.), a todos los canales (oficinas, banca online/telefónica, transacciones remotas), a todos los sistemas de soporte tecnológico y a todo tipo de clientes (minorista, mayorista). Incluye prácticas desde pagos y empleo de cheques fraudulentos hasta *phishing* o suplantación de identidad, etc.

Por tanto, la mitigación del fraude y la mejora de la ciberseguridad se encuentran entre una de las principales preocupaciones de las compañías. De acuerdo con el *G7 Cyber Expert Group*¹⁸, el objetivo principal es identificar aquellas prácticas que representan un posible fraude. Las pérdidas por coste de oportunidad (transacciones normales clasificadas como potencialmente fraudulentas) o falsos positivos deben minimizarse, pues en el caso del fraude este tipo de error presenta un impacto negativo muy elevado en la percepción que los clientes tienen sobre la compañía.

Sector asegurador

En este sector destacan los delitos asociados a los seguros del hogar, seguros de vida, seguros laborales, seguros sobre medios de transporte y seguros médicos. Se pueden clasificar los fraudes en dos categorías¹⁹:

- ▶ **"Hard fraud"**. Tiene lugar cuando el infractor obtiene dinero ilegalmente a través de una estrategia premeditada. Puede implicar a más de una persona e incluso a una persona que trabaje para la propia compañía de seguros, que actúe de forma coordinada con el titular o el beneficiario del seguro. Este tipo de fraude se da, por ejemplo, cuando alguien provoca un accidente de tráfico de manera deliberada con el objetivo de cobrar el seguro del coche.
- ▶ **"Soft fraud"**. Tiene lugar cuando el infractor interpone una reclamación legítima, pero aprovecha la coyuntura para mentir a la compañía aseguradora sobre el daño sufrido. Este tipo de fraude se da, por ejemplo, cuando se sufre un accidente de coche de forma fortuita y el conductor reporta daños mayores de los realmente sufridos. Es el tipo de fraude que se da con mayor frecuencia.

¹⁶ Según el NIST: National Institute of Standards and Technology.

¹⁷ Fuente: Management Solutions (2015): *Data Science* y la transformación del sector financiero. Management Solutions (2014): *Model Risk Management*. Aspectos cuantitativos y cualitativos de la gestión del riesgo de modelo.

¹⁸ Fuente: Fundamental Elements of Cybersecurity for the financial sector. Octubre 2016 ("*Increasing in sophistication, frequency, and persistence, cyber risks are growing more dangerous and diverse, threatening to disrupt our interconnected global financial systems and the institutions that operate and support those systems*").

¹⁹ Fuente: Insurance Information Institute.



Sector de las telecomunicaciones

Las principales categorías de fraude en este sector pueden afectar tanto a la compañía de telecomunicaciones proveedora del servicio como al cliente que suscribe un contrato legal con la compañía de telecomunicaciones, pudiéndoles afectar tanto de forma conjunta como individualmente. Se pueden distinguir tres esquemas de fraude en función de su objetivo del fraude:

- ▶ **Incremento del tráfico de llamadas.** Este esquema emplea técnicas de simulación de acceso a la red para incrementar el tráfico de llamadas hacia ciertos destinos (donde las tarifas a pagar entre operadoras son más elevadas), de modo que operadoras ilegales se benefician de dichas tarifas.
- ▶ **Manipulación de los sistemas de información de las compañías proveedoras de servicios.** Destaca el fraude asociado a los sistemas que proveen acceso a la red o *trunking SIP*.
- ▶ **Fraude telefónico.** Incluye el envío de spam o de mensajes de texto con el objetivo de obtener datos personales de los usuarios, llamadas telefónicas a instituciones financieras suplantando la identidad de un cliente, o el colapso de la red para impedir el funcionamiento normal de una compañía o sistema.

Mención especial merecen los fraudes conocidos como *"International Revenue Share Fraud (IRSF)"*²⁰ y las técnicas de *"by pass"*²¹ ilegales de las redes.

Sector energético

En el sector energético el fraude puede producirse en múltiples actividades tales como el trading de energía, los aprovisionamientos, la gestión de proyectos, la gestión comercial, etc; si bien una parte del fraude existente en este sector se refiere al hurto de energía, a la no facturación de energía consumida (más del 80% de los eventos de fraude están relacionados con la apropiación indebida²²). En este sentido, hay que mencionar que uno de los principales problemas que impacta en la eficiencia y seguridad de las empresas de energía son las pérdidas asociadas al proceso de distribución y suministro a los consumidores. Estas pérdidas se pueden descomponer en dos categorías²³:

- ▶ **Pérdidas técnicas.** Asociadas a pérdidas que ocurren de forma natural en la red, debido a fenómenos como la disipación de potencia en las líneas de transmisión, etc. y por tanto no pueden considerarse como pérdidas debido a eventos de fraude.
- ▶ **Pérdidas no técnicas.** Asociadas al fraude energético, causadas por acciones externas al sistema de suministro de energía, que consisten principalmente en hurtos de energía, impagos de clientes y pérdidas por errores en los procesos de facturación.

²⁰ Esquemas de incremento de tráfico de llamadas en el que el beneficio es compartido por la operadora ilegal del país de destino de las llamadas y por el sujeto que se encarga de generar las llamadas, aumentando el tráfico asociado a la operadora ilegal.

²¹ Consiste en el ingreso de tráfico de llamadas internacionales a un país de forma ilegal, al solo efecto de evitar pagar las debidas tasas contables entre operadores. Se suelen emplear SIM Box o llamadas VoIP para falsear el registro del origen de la llamada.

²² Association of Certified Fraud Examiners (ACFE): Report to the nations on occupational fraud and abuse. 2016 Global Fraud Study. El análisis de frecuencia de eventos de fraude por categoría muestra que más del 80% de los casos se pueden tipificar como "Asset Misappropriation".

²³ Según Pedro Antmann: Reducing Technical and Non-Technical Losses in the Power Sector. Technical report. World Bank. Julio 2009.

La identificación y diferenciación del porcentaje de energía perdida en la distribución por motivos no técnicos es un reto que deben afrontar y resolver las compañías del sector. Se pueden distinguir tres categorías²⁴:

- ▶ Aquellas **acciones que inciden sobre la red de la compañía distribuidora**. Destacan los **enganches directos** a la red de distribución sin haber suscrito ningún contrato de suministro de energía eléctrica y las **derivaciones** en el suministro de energía hacia otros puntos o instalaciones no recogidos en el contrato.
- ▶ Aquellas **acciones que inciden sobre los equipos de medida y control tales como la manipulación de los contadores**, con el objetivo de falsear los registros de consumo y comunicar un consumo inferior al real.
- ▶ Aquellas **acciones deshonestas llevadas a cabo por los empleados de las compañías** y que afectan al **ciclo comercial**. Pueden producirse, por ejemplo, cuando no hay una correcta segregación de funciones y una misma persona registra o modifica las operaciones y autoriza los pagos o facturación asociados a las mismas.

Estos tres tipos de fraude pueden constituir una falta o delito, castigado en ocasiones con sanciones, cuyo importe depende de la cantidad de energía defraudada. En general, las empresas distribuidoras deben detectar y poner en conocimiento de las autoridades las irregularidades en la red y en los equipos (p. ej. en España las multas son competencia de las Comunidades Autónomas y se establece por ley la refacturación del importe correspondiente a seis horas de consumo diario durante un año²⁵).

Palancas de gestión

Un marco integral para la gestión del fraude daría respuesta a preguntas como:

- ▶ ¿Se deben integrar las unidades de gestión del fraude en un área?
- ▶ ¿Quién es el responsable como segunda línea de defensa del fraude interno?
- ▶ ¿Qué capacidades (modelos/sistemas) son necesarias para anticiparnos al fraude?
- ▶ ¿Qué recorrido tienen nuevas tendencias como *big data/machine learning* en su gestión?
- ▶ Etc.

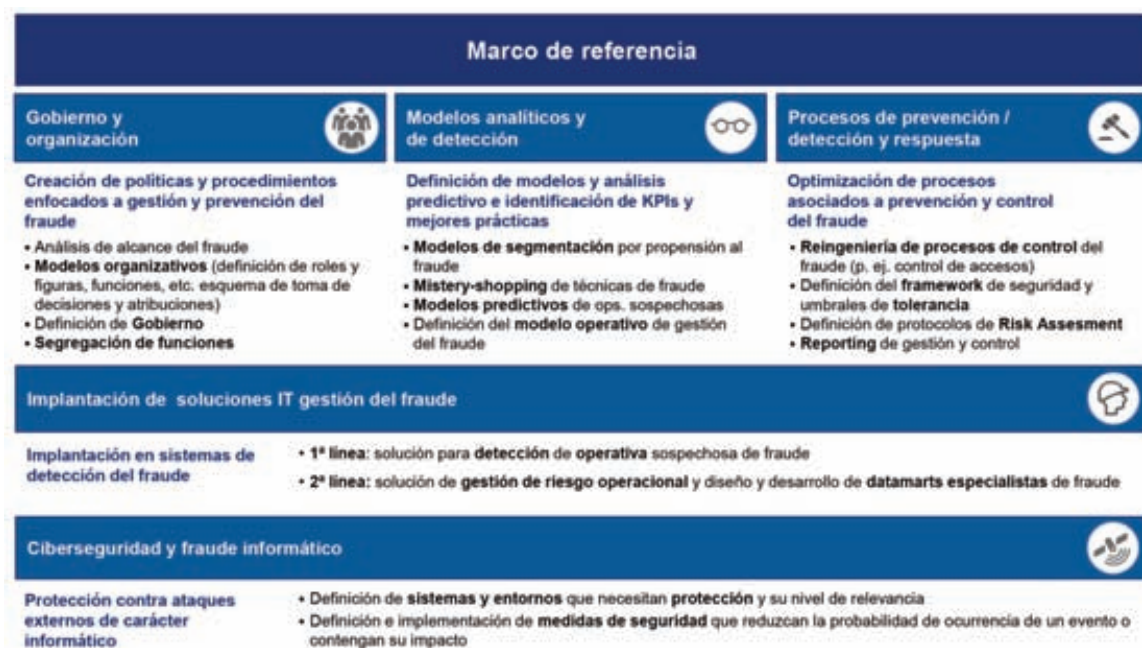
Dicho marco podría estructurarse en torno a principios/elementos básicos²⁶ tales como (véase figura 3): definición de un modelo de gobierno, establecimiento de evaluaciones periódicas del riesgo de fraude, implementación de técnicas y procesos de prevención, detección y acciones correctivas y de respuesta con las que actuar para minimizar las pérdidas una vez que el fraude ha tenido lugar. Como acciones transversales, destaca la implementación de los elementos anteriores en los sistemas y la integración de los sistemas de ciberseguridad en la operativa diaria de las compañías (para hacer frente al fraude informático, uno de los tipos de fraude más importantes y comunes, debido a la digitalización de las industrias).

²⁴ Sahoo, S., Nikovski, D., Muso, T., & Tsuru, K. (2015, February). Electricity theft detection using smart meter data. In Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society

²⁵ Según Ley 24/2013 del Sector Eléctrico.

²⁶ The Institute of Internal Auditors (IIA), The American Institute of Certified Public Accountants (AICPA) y Association of Certified Fraud Examiners (ACFE) (2012): Managing the Business Risk of Fraud: A Practical Guide.

Fig 3. Marco integral de referencia para prevenir y gestionar el fraude



Gobierno y organización

Como parte de la estructura de gobierno de una organización, las compañías establecen una política (o políticas) para la gestión del fraude que, atendiendo al origen del evento fraudulento, establece responsabilidades de gestión y control.

- ▶ Para eventos de fraude con **origen externo** es habitual que la identificación y gestión se haga desde las propias unidades de negocio a través de la aplicación de las políticas antifraude en sus procesos operativos. Paralelamente, y sin una dependencia del negocio, la supervisión de la correcta aplicación de estas políticas se lleva a cabo desde las áreas de control de riesgos, control interno y auditoría, y funciones de segunda y tercera líneas de defensa.
- ▶ Para eventos de fraude con **origen interno**, sin embargo, su identificación y gestión se hace a través de áreas independientes del negocio, como control interno o auditoría, desde donde se llevan a cabo las correspondientes investigaciones para llegar a conclusiones que permitan la toma de medidas disciplinarias. De hecho, según el Instituto de Auditores Internos de España²⁷, *“Auditoría Interna debe asegurar al Consejo y a la dirección que los controles en materia de fraude son suficientes para cubrir los riesgos identificados y garantizar que dichos controles funcionan de manera eficaz”*. Estas funciones, aparte de establecer sus procesos de monitorización, cuentan habitualmente con canales de denuncia interna anónima.

A la hora de definir las políticas antifraude, las organizaciones consideran el nivel de complejidad y profundidad que quieren alcanzar, siendo un factor relevante el tamaño de la propia compañía.

Inteligencia analítica

Según el Institute of Electrical and Electronics Engineers, la probabilidad de detección del fraude depende de la cantidad robada y del nivel de inversión realizado en dicha detección²⁸. Se debe por tanto **evaluar periódicamente la exposición** de la organización al riesgo de fraude, identificando posibles nuevas estrategias de fraude y eventos que deben ser mitigados por parte de la compañía. Además de identificar los riesgos, se debe **revisar la probabilidad de ocurrencia y su severidad** en caso de que el evento de fraude tuviera lugar.

Basados en el triángulo del fraude representado en la figura 1, se realiza una revisión de los riesgos y una definición de los indicadores analíticos para su seguimiento en informes que permitan identificar y anticipar la pensión al fraude.

La gestión del fraude, debido a su carácter adaptativo, requiere de sistemas inteligentes y de análisis estadístico para su detección. Las técnicas que permiten detectar las nuevas estrategias y patrones empleados por los infractores sin perder vigencia en el tiempo combinan **elementos puros de análisis y modelización** como *data mining* y *machine learning*, **elementos**

²⁷ IAIE: Gestión del Riesgo de Fraude: Prevención, detección e investigación. Febrero 2015.

²⁸ Fuente: Amin, Saurabh, Galina A. Schwartz, Álvaro A. Cardenas, and S. Shankar Sastry. “Game-Theoretic Models of Electricity Theft Detection in Smart Utility Networks: Providing New Capabilities with Advanced Metering Infrastructure.” IEEE Control Systems 35, no. 1 (February 2015).



técnicos de computación de alto rendimiento como *stream computing* y, finalmente, **procesos completos de transformación de datos** para la adquisición de conocimiento útil como *knowledge discovery in database* (KDD). Estos métodos deben ser empleados de forma anterior a la aplicación de los controles internos (véase fig. 4).

Algunos beneficios de emplear análisis estadístico de los datos son²⁹:

- ▶ **Visión holística de una compañía.** Cartera de clientes activos para los cuales se integran múltiples fuentes de datos (internas y externas) con la posibilidad de enriquecer la información interna fruto de la relación con el cliente (comportamiento de pago, incidencias, consumo, etc.) con información externa proporcionada por terceros (poder adquisitivo, morosidad, nivel socioeconómico, etc.).
- ▶ **Análisis de información desestructurada.** Datos provenientes de redes sociales, conversaciones, etc. representan una información valiosa a la hora de detectar el fraude; sin embargo las bases de datos tradicionales no permitían su almacenamiento de forma apropiada. Las nuevas técnicas permiten un correcto almacenamiento de estos datos, así como su explotación e incorporación a los modelos predictivos.

No obstante, los eventos no obvios y con escaso número de incidencias se deben identificar y tratar con un criterio de negocio o política definida.

En último lugar se debe llevar a cabo la validación de los modelos analíticos de fraude; es decir se debe definir e implementar el proceso de supervisión de los modelos con el objetivo de confirmar que el modelo final tiene una performance constante y

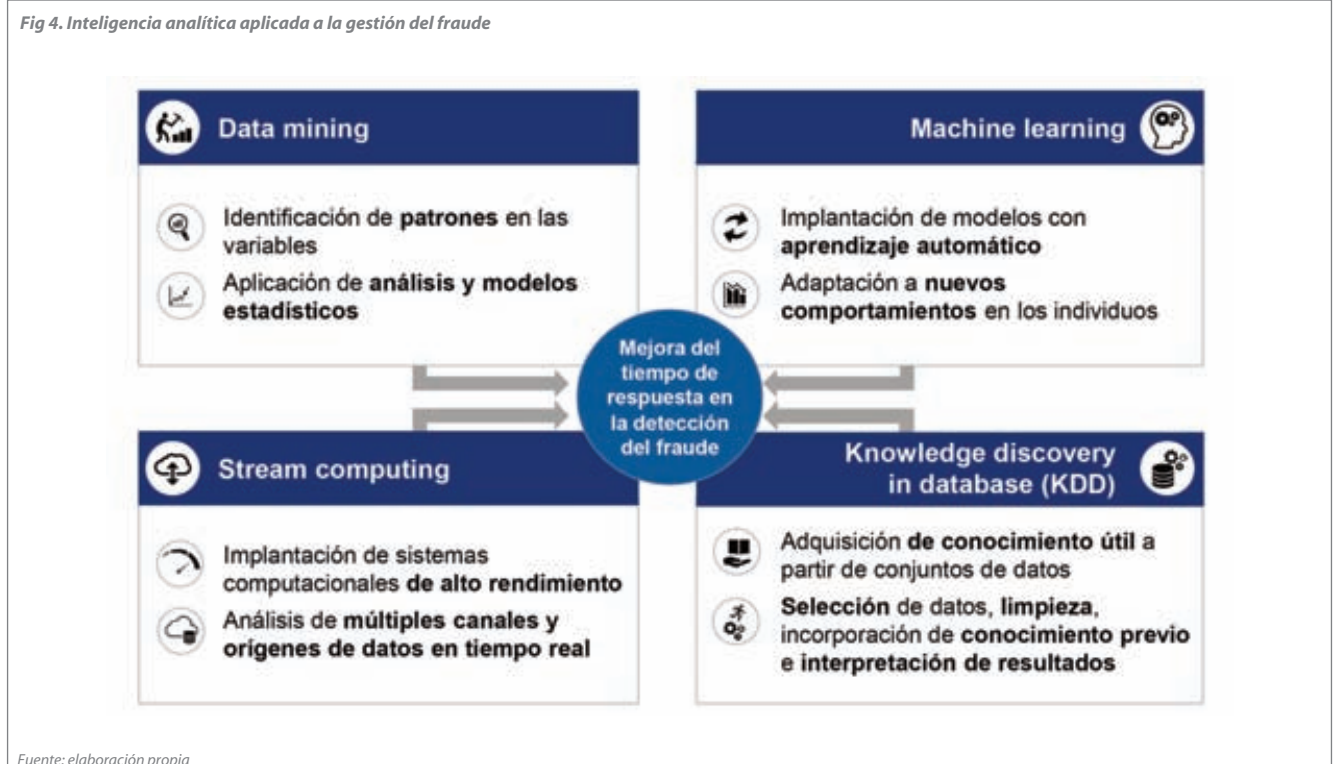
correcta, además de que cumple con los requerimientos de negocio y, potencialmente, regulatorios.

Mecanismos de prevención, detección y respuesta

Desde el punto de vista operativo, las actuaciones están orientadas a la **prevención y detección** de potenciales eventos fraudulentos (implantación de técnicas de detección de los eventos fraudulentos que no han sido previstos por los sistemas de la compañía), así como a la definición de procesos de **respuesta** para asegurar que el posible fraude se aborda de forma apropiada y a tiempo con el objetivo de minimizar la pérdida asociada al evento fraudulento.

- ▶ **Identificación** mediante la definición de qué procesos, datos, sistemas y entornos necesitan protección y su nivel de relevancia;
- ▶ **Protección** a través de la implantación de controles, ya sean sistemas u operativas de control, que reduzcan ex ante la exposición al riesgo o impidan que una amenaza se convierta en fraude (p. ej. políticas de accesos);
- ▶ **Detección** mediante sistemas de alerta temprana que, a través de la monitorización o análisis, permitan la identificación de la ocurrencia de un fraude u operativa fraudulenta (p. ej. cuadro de mando de KPIs/KRIs); y
- ▶ **Respuesta y recuperación** utilizando procesos ágiles de puesta en marcha de medidas correctivas para minimizar

²⁹ Un ejemplo de aplicación práctica de estos beneficios se puede encontrar en Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. Decision Support Systems, 46(4).



y/o subsanar las pérdidas causadas por el evento fraudulento (reducir su impacto).

- ▶ **Reportar** tanto los niveles de fraude de la organización como la gestión realizada y pérdida sufrida.

Modelo de soporte tecnológico

La implementación de los elementos anteriores en los entornos tecnológicos de las organizaciones es clave para la gestión del fraude³⁰:

Un sistema integrado de prevención y detección del fraude facilita la gestión de todos los procesos de negocio impactados por este riesgo. Las características básicas de un sistema de detección del fraude son las siguientes:

- ▶ Disponer de un **repositorio de datos con toda la realidad de fraude de la organización**. Debe contar tanto con las variables de entrada a los modelos de detección como con las puntuaciones obtenidas en la ejecución de los modelos sobre la actividad transaccional de la organización y las alertas generadas. Implementa **controles de calidad de datos** tanto en el histórico como en la captura de nuevas variables.
- ▶ Implementar un **modelo de detección del fraude parametrizable y adaptable** a la problemática de la organización. Generalmente, estos sistemas cuentan con modelos pre-parametrizados basados en el conocimiento de la industria que deben ser particularizados y monitorizados (su desempeño).
- ▶ Implementar **flujos de generación de alertas e informes dinámicos** de acuerdo con el esquema de revisión y análisis implantado en la organización para la definición de alertas en modo *on-line* o *batch*.

Para que un sistema de detección del fraude se integre eficazmente en la gestión tiene que facilitar el aprovisionamiento de la **información transaccional y comercial** de los clientes; su integración *on-line* (p. ej. vía servicios *web*) en los procesos de autorización / denegación de actividad transaccional; presentar un **alto rendimiento tecnológico** por su involucración en procesos con interacción con cliente; disponer de un **sistema de autenticación compatible** con los estándares organizacionales (p. ej. LDAP); y contar con un **esquema de roles y usuarios definible** de acuerdo con las políticas de la organización.

Con el objetivo de ilustrar la integración de un sistema de detección del fraude dentro del entorno tecnológico de una organización, en la figura 5 se muestra un ejemplo del ciclo de vida de la información analizada en el proceso de detección del fraude: desde el lanzamiento del evento de originación por parte del cliente y su entrada en el procesamiento interno de la organización hasta la decisión final relativa a la sospecha de actividad relacionada con fraude.

De igual forma, se muestra la jerarquía funcional de los diversos componentes internos de dicho sistema: desde el almacenamiento de la información granular en el repositorio de datos hasta la ejecución de los modelos de detección del fraude con la información transaccional recibida y la posterior gestión de las alertas y su *reporting*.

³⁰ "The results of Data Analytics may be used to identify areas of key risk, fraud, errors or misuse; improve business efficiencies; verify process effectiveness; and influence business decisions.", ISACA, Information Systems Audit and Control Association: Data Analytics – A practical approach. White Paper. August 2011.

Fig 5. Integración de un sistema de detección del fraude



Técnicas de gestión del fraude en el sector energético



El incremento de la capacidad de almacenamiento de información y la potencia de cálculo ha impulsado el desarrollo de la **Inteligencia Analítica**, así como de las diferentes disciplinas que engloba, entre las que destaca el **Data Science**, cuyo objetivo es extraer el máximo conocimiento de los datos, combinando análisis de información masiva con técnicas de modelización, perfilación y segmentación³¹.

En el sector energético, estas técnicas se emplean para afrontar problemáticas que van desde la predicción de la demanda energética hasta la identificación de patrones de consumo con el objetivo de realizar ofertas comerciales personalizadas o detectar eventos de fraude.

Datos

La recopilación y posterior tratamiento de datos conlleva un análisis previo de su tipología, naturaleza y origen de los mismos (véase figura 6).

En todo caso, localizar las fuentes, determinar los procesos de extracción, almacenamiento y procesamiento, analizar la calidad de los datos, etc., son actuaciones que requieren ser

realizadas al amparo de un marco de gobierno de datos, aprobado por el primer nivel de la compañía.

Dicho gobierno de datos implica desarrollar tres dominios: i) Arquitectura tecnológica, ii) Personas y sus capacidades, iii) Procesos / Instrumentos para llevar a cabo un gobierno efectivo (véase figura 7).

La clave en el gobierno del dato está en hacer de él un instrumento útil para la gestión. En este sentido procede primero identificar y delimitar los datos a gestionar y después clasificarlos en función de su tipología (internos, externos, estructurados, no estructurados, etc.) y del nivel de protección requerido.

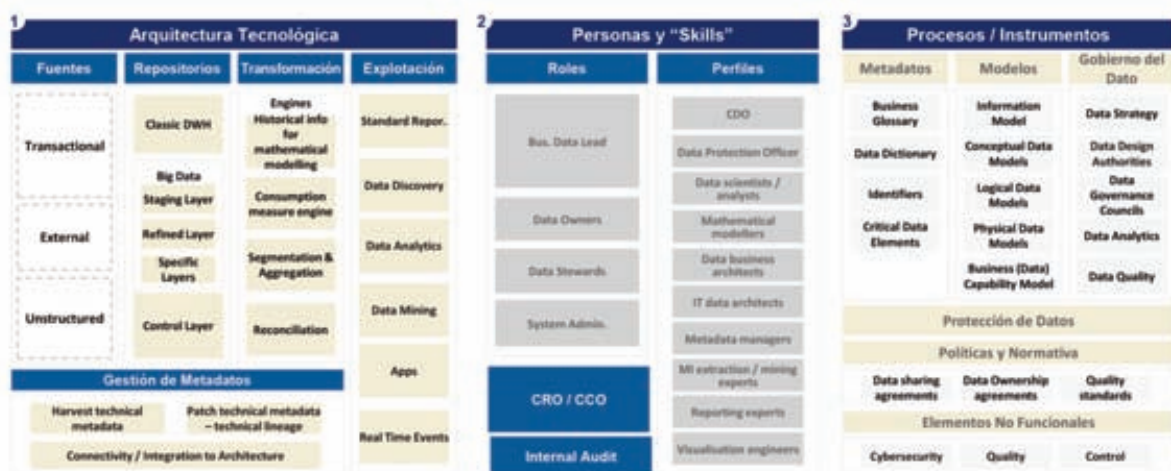
Con todo ello se debe establecer una **priorización** de los datos atendiendo principalmente al coste/beneficio de un mayor o menor gobierno sobre la información y, finalmente, desarrollar un marco enfocado a la **formalización** (definición de los conceptos, *owners*, fuentes de información, etc.), **seguimiento**

³¹ *Data Science* y la transformación del sector financiero. Management Solutions (2015)

Fig.6. Principales bloques de información en corporaciones



Fig.7. Dominios de desarrollo para el gobierno del dato



Fuente: elaboración propia

de calidad y planes (controles e indicadores para seguimiento de calidad, planes de remediación, etc.) y **validación** independiente (certificación o auditoría interna) considerando los aspectos relacionados con la protección de la información tanto interna, como de clientes (GDPR³²).

Modelos

Los modelos a desarrollar pretenden encontrar patrones, tendencias o reglas que expliquen el comportamiento del cliente, empleado o un tercero antes de la detección del fraude.

A la hora de seleccionar las variables a incluir en el modelo, se debe garantizar que estas cumplan las siguientes condiciones:

- ▶ Cubran todos los perfiles que funcionalmente se desean reflejar.
- ▶ Aporten el mayor poder predictivo conjunto y no sean redundantes.

Para ello, se realiza un análisis estadístico de las variables (univariante y multivariante), incluyendo análisis para detectar la multicolinealidad, a través del estudio de la correlación entre las variables explicativas. Con esto se logra mayor simplicidad en el modelo.

Entre las herramientas estadísticas y numéricas más utilizadas para analizar y corregir la correlación se encuentran el uso de indicadores estadísticos (como el coeficiente de correlación de Pearson, Kendall o Spearman, según el tipo de variables), o el empleo de técnicas de reducción de la dimensionalidad, como el análisis de componentes principales (PCA por sus siglas en inglés), en el que se busca un subespacio dimensional inferior sobre el que proyectar los datos, minimizando los errores de proyección.

Una vez acotado el conjunto final de variables explicativas, se procede a la construcción del algoritmo. Las técnicas a emplear para la identificación de los perfiles/observaciones susceptibles de representar un evento de fraude variarán en función del fin perseguido y del tipo de dato utilizado. Destacan las siguientes metodologías:



- ▶ **Modelos de clasificación.** El objetivo de este tipo de metodologías es predecir la clase a la que pertenece cada una de las observaciones o registros que se pretenden analizar en función de sus atributos. Algunas de las técnicas más empleadas son los árboles de decisión, los cuales pueden ser generados a través de diferentes algoritmos como CLS, ID3, CART, etc. La técnica de **Random Forest** constituye otro tipo de modelo de clasificación que se basa en la agregación de varios árboles de decisión (p. ej. usando la moda o la media) para predecir la clase a la que pertenece cada registro.

Otras técnicas de clasificación comúnmente empleadas son los **Clasificadores Bayesianos**, las **Redes Neuronales** o la **técnica k-Nearest Neighbours**.

- ▶ **Modelos de regresión.** El principal objetivo es la estimación numérica de la relación entre una variable dependiente y un conjunto de variables explicativas. Existen dos tipos de regresiones, **lineales y no-lineales**. Ejemplos de este tipo de modelos son las **regresiones lineales Bayesianas** y los **modelos lineales generalizados (GLM)**. Las **regresiones logísticas** constituyen un modelo de regresión cuya finalidad es la

³² General Data Protection Regulation. Nuevo marco normativo para la Unión Europea, (tanto para las relaciones entre estados miembros como con terceros) en materia de protección de la información con el objetivo de armonizar y unificar criterios en la aplicación y garantía de los derechos en materia de privacidad y protección de datos, adaptando los estándares al entorno digital.

Fig.8. Algunas metodologías aplicadas a la detección del fraude

MODELOS DE PREDICCIÓN	Ventajas	Inconvenientes	Clientes positivos (con ocurrencia del evento) Clientes negativos (sin ocurrencia)
<p>Redes Neuronales</p> <p>Función no lineal que permite discriminar los clientes positivos de una población dada.</p> <p>A menudo resulta un modelo complejo y no permite una interpretación sencilla e intuitiva de sus parámetros.</p>	<ul style="list-style-type: none"> • Permite capturar relaciones no lineales entre variables. • Elevada capacidad predictiva sobre una muestra dada. 	<ul style="list-style-type: none"> • Riesgo de "sobreentrenamiento" y pérdida de poder predictivo sobre la muestra de test. • No interpretabilidad del comportamiento explicativo de las variables. 	
<p>Árboles de decisión</p> <p>Modelo de predicción basado en la aplicación secuencial de reglas excluyentes y que a cada partición final asocia una probabilidad.</p> <p>La partición que genera el árbol determina regiones por rectas paralelas a los ejes lo que resulta en una limitada capacidad discriminante del modelo.</p>	<ul style="list-style-type: none"> • Fácilmente interpretable. • Permite identificar segmentos de mayor densidad. 	<ul style="list-style-type: none"> • No permite capturar el efecto combinado de variables predictivas. 	
<p>Regresión logística</p> <p>Modelo lineal generalizado que determina la probabilidad de un evento como función de otros factores mediante una función logística.</p> <p>Determina la frontera que discrimina el evento de ocurrencia (a mayor grado de ajuste más precisa será la discriminación).</p>	<ul style="list-style-type: none"> • Permite capturar el efecto conjunto de variables. • El resultado es interpretable como una probabilidad de acierto (comportamiento monótono de las variables explicativas). • El efecto de cada variable en el modelo es interpretable. 	<ul style="list-style-type: none"> • No permite capturar relaciones no lineales entre variables. 	

Fuente: elaboración propia

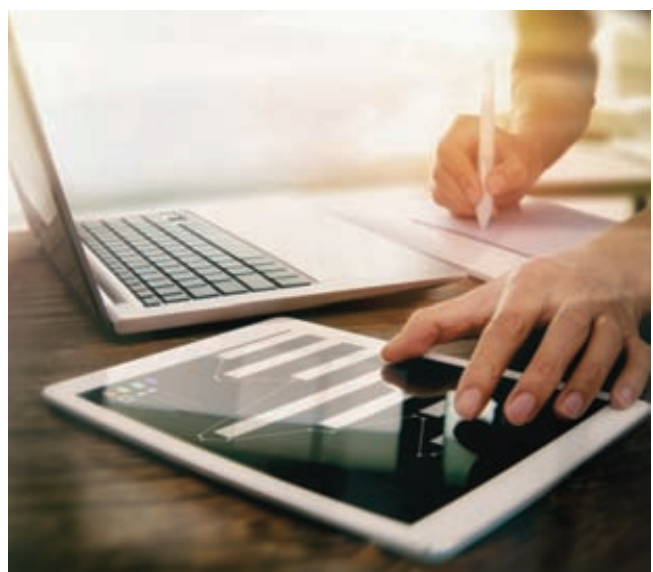
clasificación de las observaciones. El análisis mediante regresiones también se usa para realizar predicciones sobre la evolución temporal de una variable, es decir, para el análisis de series temporales. En particular, los modelos **ARIMA (Autoregressive Integrated Moving Average)** se emplean para la predicción de valores futuros de las series temporales, basándose en los valores pasados.

- ▶ **Modelos de segmentación o clustering.** El objetivo de esta metodología es la agrupación de las distintas observaciones en grupos homogéneos o *clusters*, en función del grado de semejanza que presentan. Se trata de modelos no supervisados, ya que se ajustan los datos a partir de una muestra en la que los grupos objetivos son desconocidos a priori es decir, no hay conocimiento previo sobre las clases en las que pueden quedar asignadas las observaciones. Dependiendo del criterio usado para determinar el grado de semejanza entre observaciones se distinguen distintos tipos de análisis *cluster*: **modelos de centroides (p. ej. k-means o k-medians), modelos de distribuciones estadísticas (p. ej. expectation-maximization algorithm, Gaussian Mixture Models), modelos jerárquicos** en el que los *clusters* se fusionan o subdividen sucesivamente, siguiendo una prelación o jerarquía, etc. Las técnicas de *clustering* suelen constituir un primer paso a la hora de abordar los problemas de clasificación cuando no hay información suficiente sobre las clases que se quieren diferenciar.

Otras técnicas que se emplean en la detección del fraude son las **reglas asociativas (associative rules o ARs), la identificación de secuencias (Motif Mininig, Autocorrelation Function) o la detección de anomalías u outliers.** Cada uno de los tipos de modelos muestra diferente grado de capacidad predictiva, estabilidad e interpretabilidad.

El aprovechamiento completo de todo el potencial que representan las técnicas de *Data Science* conlleva la implementación de las siguientes características en algunos de los procesos que conforman el ciclo de vida de los modelos:

- ▶ **Análisis en tiempo real.** Los sistemas de recopilación de información permiten llevar a cabo la captura y seguimiento de los datos en tiempo real. Además, es posible programar algoritmos que hagan uso de dicha información, lo que facilita y agiliza la detección de los nuevos patrones y estrategias de fraude no empleadas hasta ese momento por los infractores. Además, esta característica hace que los modelos no pierdan poder predictivo con el paso del tiempo, estando siempre actualizados y siendo sensibles a los nuevos patrones de fraude.
- ▶ **Reentrenamiento automático y autoaprendizaje.** Los modelos de detección del fraude son recalibrados de





forma automática (con escasa intervención de los analistas) e iterativamente a partir de los grandes volúmenes de datos, lo cual se traduce en una potencial mejora del poder predictivo durante los sucesivos reentrenamientos.

El análisis en tiempo real, el reentrenamiento automático y el autoaprendizaje de los modelos reduce el *time-to-market* de los mismos. Además, estas características posibilitan la búsqueda y detección de patrones y relaciones sin restricciones predefinidas y de forma actualizada, así como la identificación e incorporación a los modelos de nuevas variables relevantes. También es posible programar los modelos de forma que se recalibren de forma automática a través de la variación en los pesos relativos con los que contribuye cada variable a la detección de los eventos de fraude.

Por contrapartida, esta sofisticación de los procesos conlleva una mayor complejidad en la gestión del riesgo de modelo, siendo necesaria la implementación de controles internos y sistemas de alertas que permitan detectar cualquier desviación del modelo, así como controles sobre los grados de libertad en la automatización de procesos. Todo ello debe ir acompañado de un marco de gestión de modelos.

Principales ámbitos de aplicación en la gestión del fraude del sector energético

A continuación se tratan dos ámbitos específicos de aplicación en el sector energético: aquellos relacionados con el **hurto de energía en la red de distribución** y aquellos vinculados a las **actividades fraudulentas en el ciclo comercial**. Estos ámbitos son relevantes tanto por su impacto económico (se estima que a nivel mundial las utilities llegan a perder más de 95 billones de dólares anualmente por pérdida no técnica de energía³³) como reputacional (p. ej., incremento de la diferencia entre la demanda eléctrica medida en los puntos de consumo y la energía medida en las centrales de generación, ocasionando sobrecostes para el sistema que repercuten en los consumidores³⁴). El primero de ellos gira en torno a la cuantificación de la propensión o probabilidad del uso de energía por parte de un cliente o usuario sin constancia por

parte de la compañía (fraude externo). El segundo a la identificación de incompatibilidades en procesos, como el ciclo comercial, que pueden generar lucro a empleados (fraude interno).

Fraude externo: hurto de energía

El aumento en la **capacidad de generar y almacenar información** puede ser aprovechado para tener acceso en tiempo real a la caracterización de un cliente, una operación, un proceso, etc., lo cual se utiliza para **identificar comportamientos indicativos de propensión a la existencia de hurto de energía**.

Desde hace años, la detección de las **pérdidas no técnicas** ha supuesto una de las principales preocupaciones de las compañías. Sin embargo, las soluciones históricamente implicaban elevados costes (inspecciones por parte de técnicos).

Hoy en día, en numerosos países se están desarrollando e implementando las conocidas como Infraestructuras de Medición Avanzada o AMI³⁵ en las *Smart Grids*³⁶, que incluyen sistemas de recopilación de datos y monitorización en tiempo real, así como el uso de técnicas de análisis basadas en inteligencia artificial, teoría de juegos, etc.

De acuerdo con los resultados obtenidos del estudio desarrollado por el Departamento de Energía de Estados³⁷ Unidos, el empleo de estas técnicas de *Data Science* para la detección del fraude en el sector energético resulta de gran utilidad a la hora de diferenciar el porcentaje de energía

³³ Electricity Theft and Non-Technical Losses: Global Markets, Solutions, and Vendors. Mayo de 2017, Northeast Group, LLC.

³⁴ Informe sobre las alternativas de regulación en materia de reducción de pérdidas y tratamiento del fraude en el suministro eléctrico. Informe de 16 de julio de 2015 de la CNMC, Comisión Nacional de los Mercados y la Competencia.

³⁵ Advanced Metering Infrastructure.

³⁶ Redes eléctricas inteligentes.

³⁷ US Department of Energy – Office of Electricity Delivery and Energy Reliability: AMI and Customer Systems: Results from the SGIG Program. Septiembre 2016.

perdida en la red de distribución asociado a pérdidas técnicas (no representativas de un evento de fraude) y a pérdidas no técnicas (hurto de energía y por tanto representativas de un evento de fraude).

Asimismo, las compañías energéticas están llevando a cabo campañas de implementación de contadores inteligentes SM³⁸ que ayudan a reducir las pérdidas no técnicas en su red de distribución³⁹. Según el Departamento de Energía de Estados Unidos⁴⁰, la recopilación de los datos de consumo mediante estos dispositivos junto a su posterior análisis mediante el empleo de técnicas de tratamiento de grandes volúmenes de datos ofrece nuevas posibilidades para el desarrollo de métodos eficientes y efectivos de detección de fraude, mejorando la recuperación de ingresos. Algunos de los beneficios del empleo de SM son la posibilidad de lectura de los datos de consumo en remoto, la mayor resolución de las mediciones, así como la detección de **cortes o desconexiones no previstos** en el proceso de recopilación de datos por parte del contador.

No obstante, su uso también presenta diversos retos:

- ▶ La recopilación de datos durante largos periodos de tiempo debido a limitaciones en la capacidad de **almacenamiento**.
- ▶ La existencia de procesos de compresión que reducen la **calidad del dato** y limitan las posibilidades de utilización posterior.
- ▶ El coste computacional del **procesamiento en tiempo real**.
- ▶ La protección de la información privada sujeta a restricciones de **confidencialidad**⁴¹.

La inversión en modelos de detección avanzados **optimiza las tasas de éxito de las campañas de inspección** y mejora la detección del fraude. Si bien avanzar en la implantación de este tipo de modelos requiere previamente definir e implementar un marco de referencia que facilite el gobierno de los datos, modelos y procesos asociados (véase fig. 9).

El proceso objeto de análisis consiste en la **ejecución de inspecciones**. Integrar en la gestión de dicho proceso, como se ha visto en los anteriores apartados, las técnicas analíticas de segmentación, requiere de un esquema de tratamiento de grandes volúmenes de información así como de perfilación de clientes.

Una vez que los modelos de segmentación han generado las probabilidades de ocurrencia del evento (en este caso la existencia de hurto de energía), estas probabilidades combinadas con el beneficio esperado de la actuación (p. ej. la cantidad de energía hurtada) ayudan a predecir el resultado esperado de una inspección.

Por tanto, para la operativización de un esquema de inspecciones de este tipo es habitual disponer de un modelo de soporte o gestor de campañas que permita aplicar los filtros y priorizaciones generados por el modelo, así como recopilar los resultados de las campañas de inspección que permitirán realimentar los propios modelos.

Esta última cuestión es de suma importancia; el resultado de una inspección constituirá un valioso *input* para la caracterización de un suministro en el futuro, ayudando a caracterizar tanto reincidentes como falsos positivos.

³⁸ Smart Meters.

³⁹ Referencia: "AMI (advanced metering infrastructure) provides powerful tools to reduce total losses and increase collection rates", publicado en World Bank: Reducing Technical and Non-Technical Losses in the Power Sector. Julio 2009.

⁴⁰ US Department of Energy – Office of Electricity Delivery and Energy Reliability: AMI and Customer Systems: Results from the SGIG Program. Septiembre 2016.

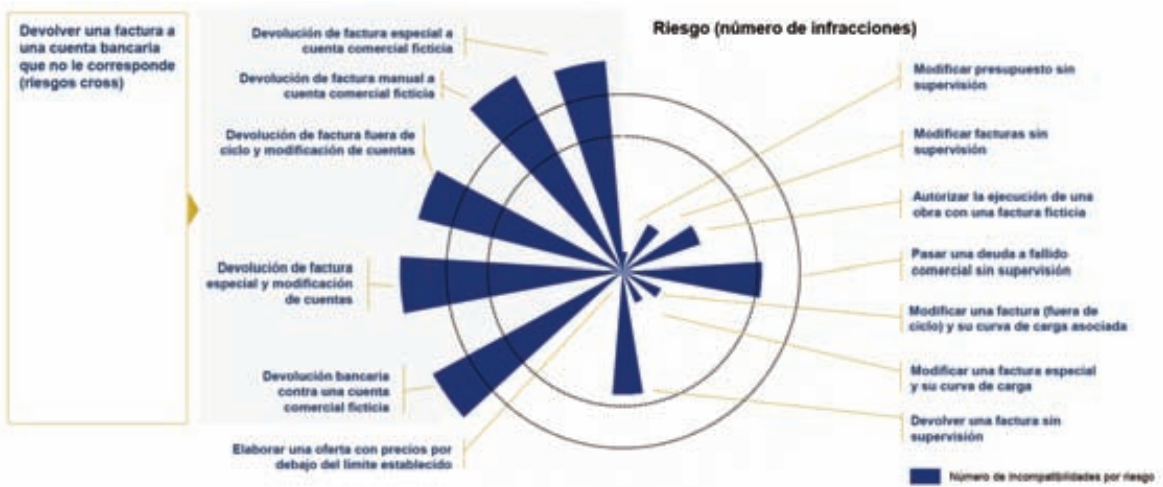
⁴¹ Se trata de datos considerados de carácter personal, y quedan sujetos a la Ley Orgánica de Protección de Datos (LOPD) y a su reglamento de desarrollo (Real Decreto 1720/2007). En ese sentido, para su explotación sería necesario el consentimiento expreso del interesado (en su caso del cliente) según su artículo 6. En las condiciones generales de los contratos de las principales distribuidoras se permite el uso de los datos por la distribuidora, y por terceros de empresas que tengan una relación contractual y solo para prospección comercial. Estos requerimientos se ven reforzados por el nuevo Reglamento General de Protección de Datos (RGPD), en el que se refuerzan los requerimientos a la gestión de consentimientos por parte del cliente (concesión explícita del uso para una finalidad y periodos concretos).

Fig.9. El empleo de las técnicas de Data Science impacta a los datos, metodología y procesos



Fuente: elaboración propia

Fig.10. Taxonomía ilustrativa de riesgos en sistemas comerciales



Fuente: elaboración propia

Fraude interno: segregación de funciones en el ciclo comercial

Las compañías energéticas disponen de múltiples sistemas para soportar sus procesos operativos. A dichos sistemas tienen acceso tanto empleados como profesionales externos.

Los cambios de posición de los empleados o la existencia de usuarios genéricos en algunos sistemas (principalmente derivados de la externalización de funciones como las áreas de facturación y cobros o *call centers*), añaden **complejidad al seguimiento de las funciones** desempeñadas por los distintos intervinientes.

La posibilidad de que un trabajador pueda realizar acciones que le permitan obtener un beneficio propio (p. ej. modificando la cuenta corriente de un cliente por la del empleado y realizando una devolución de la factura o modificando el importe de una factura del empleado y su consumo asociado), supone un **riesgo de fraude interno**.



La implantación de soluciones de control de accesos permite identificar debilidades, especialmente en los sistemas comerciales donde muchas funciones suelen encontrarse externalizadas, lo que hace que afloren multitud de riesgos relacionados con la segregación de funciones. Véase una taxonomía ilustrativa de riesgos en sistemas comerciales (figura 10).

Los proyectos de control de accesos persiguen i) revisar los roles para identificar funciones incompatibles, ii) reasignar tareas para eliminar dichas incompatibilidades o iii) en caso de no poder evitar la incompatibilidad, establecer controles de mitigación.

Muchas empresas energéticas han implantado soluciones de control de accesos (también conocidos como *Access Control* o *Identity Management*) con un triple objetivo:

- ▶ **Reducir el riesgo de accesos no autorizados** a los sistemas mediante la definición de un modelo de *user provisioning* que realice un control *ex ante* que permita anticipar situaciones de incompatibilidad (antes de conceder un rol a un usuario se verifica que dicha concesión no supondrá un incumplimiento con la SoD).
- ▶ **Garantizar la confidencialidad, la integridad y la disponibilidad de la información mediante la segregación de funciones**, asegurando que los accesos a información crítica de la empresa se encuentra controlada y solo acceden las personas adecuadas (p. ej. sistemas de nóminas o sistemas contables).
- ▶ **Automatizar el *user provisioning***, garantizando que los empleados disponen de los permisos requeridos en el menor tiempo posible (p. ej. automatización del acceso a sistemas en función del puesto de trabajo y eliminación de accesos cuando se produzcan bajas o cambios de área en la compañía).

Fig.11. Identity Management



Fuente: elaboración propia

El control de la identidad y acceso (denominado *Identity Management*) engloba tres procesos principales (*User Lifecycle Management*, Autenticación y Autorización) que garantizan que los usuarios i) son quienes dicen que son y ii) acceden a las aplicaciones adecuadas con los derechos necesarios.

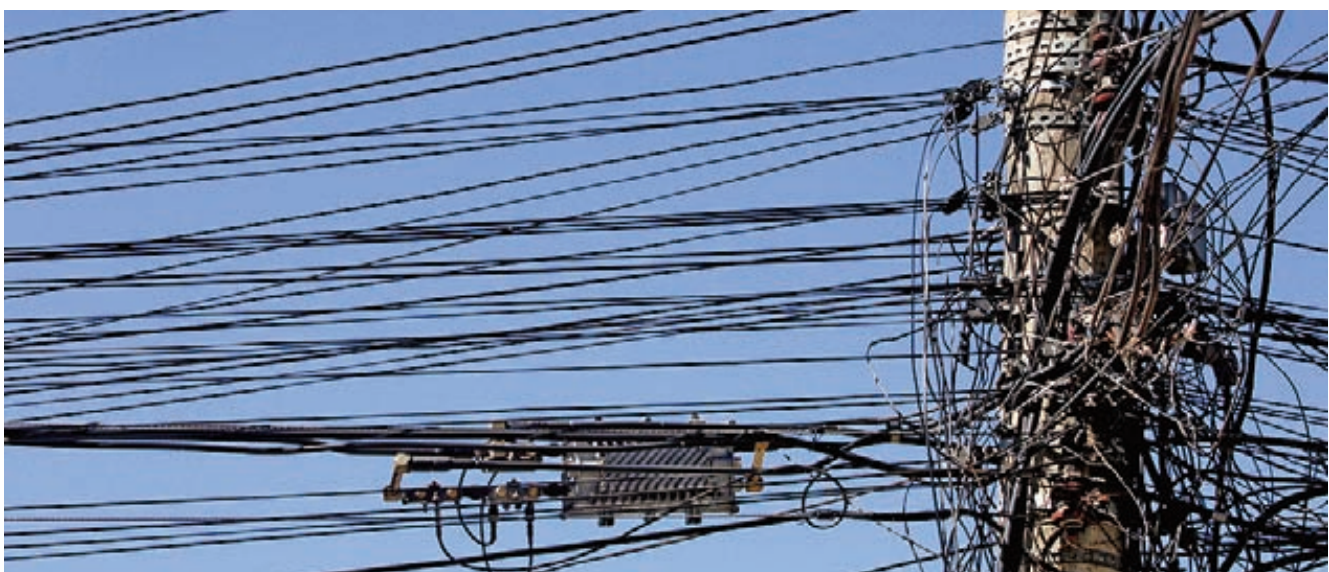
Estos procesos son sustentados en soluciones tecnológicas (conocidas como IGA: *Identity Governance and Administration*) cuya implantación permite a las compañías incrementar el **nivel de control** sobre los accesos a los sistemas garantizando la segregación de funciones, disminuyendo por tanto el riesgo interno de la compañía. Si bien estas soluciones requieren de una monitorización continua para garantizar el correcto control de la segregación de funciones, así como disponer de herramientas de análisis que permitan definir:

- ▶ **Un plan de medidas o controles de mitigación para las incompatibilidades**, como la remediación de roles/usuarios o el establecimiento de excepciones que

sean monitorizadas con controles mitigantes (p.ej. definir informes o procesos para garantizar el control sobre el riesgo).

- ▶ **Un protocolo de actuación** para que los riesgos e incompatibilidades que se pongan de manifiesto en futuras revisiones sean resueltos o mitigados con rapidez.

En todo caso, el control efectivo de los accesos puede verse comprometido si no se dispone de una visión global de los accesos del empleado y autorizaciones independientes por aplicativo, así como de procesos para la supresión de dichos accesos (p. ej. cuando un empleado cambia de posición en la empresa, no siempre se eliminan los permisos que requería en su antigua posición). Igualmente importante resulta realizar análisis de riesgo por puesto, antes de cancelar un acceso.



Ejemplo de aplicación de técnicas de modelización: hurto de energía



La detección del fraude energético, asociado al consumo ilegal de energía en la red, parte de una segmentación de los **clientes basada en su probabilidad de cometer fraude**. Para ello, se interpretan los datos históricos de fraude y su impacto en el negocio, así como el comportamiento histórico de los hurtadores (entre otros el resultado de inspecciones previas, facturación y cobro).

Las técnicas de modelización aplicadas en la gestión de la detección del fraude energético persiguen mejorar la tasa de éxito en la selección de clientes a inspeccionar.

Ciclo de vida de los modelos de detección

Los modelos utilizados en la detección del fraude pasan por cuatro etapas: extracción de la información, análisis estadístico de los datos, construcción, y validación y certificación (véase figura 12).

Extracción y tratamiento de los datos

En la primera etapa de extracción y tratamiento de la información de los clientes de energía se distinguen a su vez varias fases: la solicitud y extracción de los datos, el análisis de la calidad de la información y la construcción de nuevas variables (véase fig. 13).

La información recogida quedará registrada en una tabla única. Además se crearán nuevas variables a partir de los datos capturados. La selección de variables relevantes con buen poder predictivo para la detección del fraude energético requiere de un profundo análisis estadístico. Algunas variables que han demostrado un alto poder predictivo son:

- ▶ **Datos del medidor:** el tipo de conexión (monofásico, bifásico o trifásico), la marca y modelo del medidor pueden ser relevantes por la complejidad de manipulación para el fraude y representar una oportunidad percibida por el cliente. Otras variables relevantes pueden ser el tipo de red y la potencia instalada del medidor que define el posible consumo máximo del cliente, ya que su relación con el consumo real debería tener valores próximos en un cliente sin fraude.
- ▶ **Datos sociodemográficos:** estos datos pueden ser útiles para segmentar la población. Por ejemplo los atributos de localización (comunidad, provincia, ciudad, municipio, código postal, barrio o región), donde se aprecian altos poderes explicativos del evento de fraude. Para complementar la información del cliente, se puede obtener información externa enriquecida por zonas, como renta media, consumo medio, tipos de vivienda, clima, etc.
- ▶ **Datos del cliente:** en general las empresas de energía disponen de información útil del cliente (antigüedad,

Fig.12. Etapas en la creación de un modelo

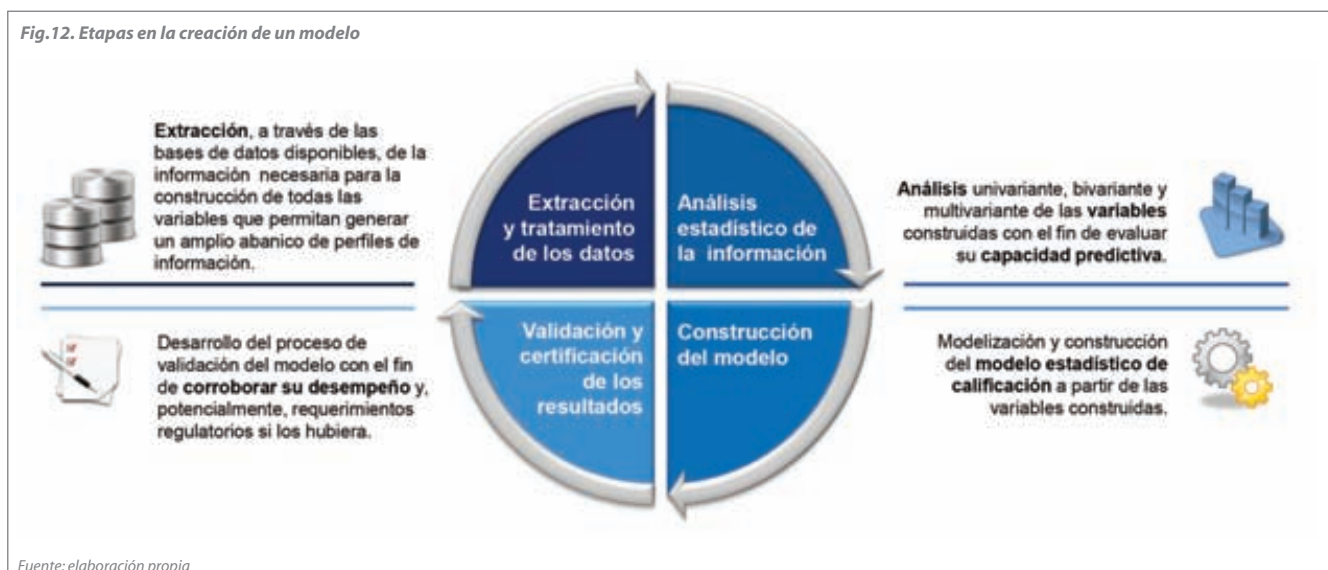
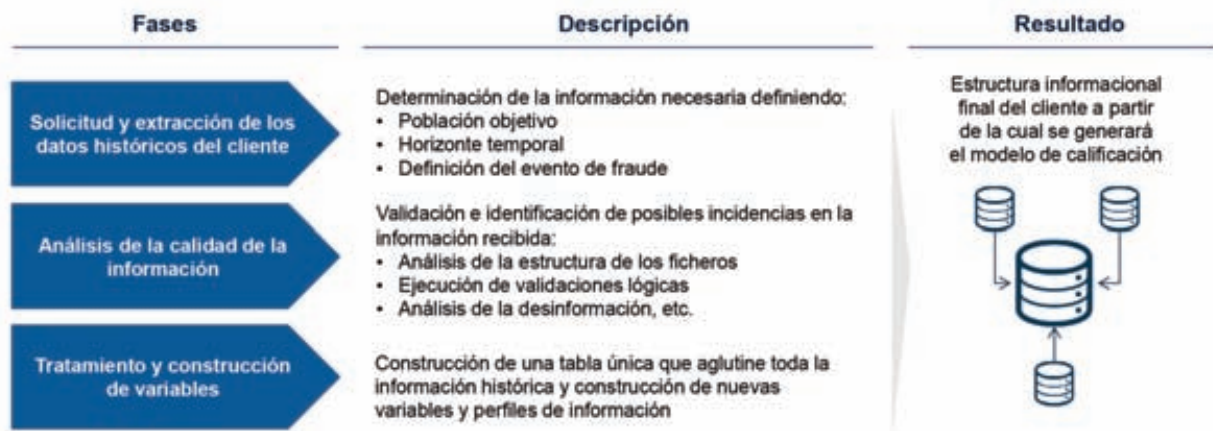


Fig.13. Tratamiento de los datos en la construcción de un modelo



Fuente: elaboración propia

consumo colectivo o individual, clase del cliente: residencial, empresa, industrial, servicio público, rural, luz pública, cliente de baja renta, etc.). En el caso de grandes clientes se incrementa el volumen de información disponible con atributos como la actividad, industria, etc.

- ▶ **Datos de consumo** histórico de la energía: esta información juega un papel fundamental para analizar el comportamiento del cliente y gracias a la teled medida la calidad de estas variables ha mejorado sustancialmente en los últimos tiempos. Cabe destacar el análisis de la desviación en el consumo esperado por motivos cíclicos, climatológicos, cortes de energía u otros, con respecto a clientes semejantes o al mismo cliente en periodos pasados; así como irregularidades en las lecturas del contador, periodicidad en las lecturas del cliente, deuda, etc.

La frecuencia y variedad de esta información va enriqueciéndose cada año (históricamente se podría disponer de una escasa información, como consumo trimestral de un punto de suministro comunitario, si bien hoy en día se puede obtener, con los teled medidores inteligentes, información detallada de corrientes, fases, tensión, potencia, etc. en tiempo real).

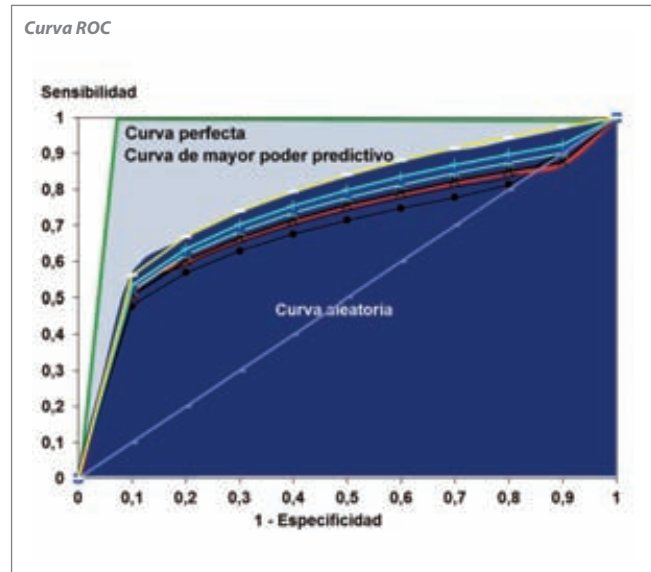
- ▶ **Datos de la operación o gestión realizada:** Datos de la operación de mantenimiento de la red y de los medidores, información de cortes e irregularidades o información de contactos o reclamaciones con el cliente, etc., son informaciones que pueden ser útiles.
- ▶ **Datos de la inspección:** el detalle del resultado de la inspección no puede ser usado como variable para el modelo, pero sí ayuda a realizar un análisis previo de las causas que originan un fraude. En el subconjunto de clientes reincidentes, se puede usar alguna información que rápidamente identifique el nuevo fraude.

Análisis estadístico de la información y construcción del modelo

En primer lugar se realiza un análisis estadístico de la información para detectar las variables más relevantes, según se ha expuesto en el apartado de Factores subyacentes al fraude. Se dispone al llegar a esta etapa de una batería de variables depuradas de errores y potencialmente predictivas del fraude del cliente, por lo que se puede proceder a la construcción (calibración) del modelo⁴². A continuación, se **selecciona el algoritmo** más apropiado para el modelo que se desea construir sobre la población de estudio y se determinan sus parámetros. Opcionalmente, la asignación de pesos a las variables (seleccionadas mediante técnicas estadísticas) permite perfilar y **discriminar clientes** de comportamientos asimilables al fraude.

Desde el punto de vista estadístico podemos distinguir dos enfoques diferentes al problema de clasificación. En el primero de ellos, los grupos están bien definidos y se trata de determinar un criterio para etiquetar cada individuo como perteneciente a alguno de los grupos, a partir de los valores de una serie limitada de parámetros. En este caso, las técnicas más utilizadas se conocen con el nombre de **análisis discriminante**, aunque existen otras posibles alternativas, tales como la utilización de la regresión logística, redes neuronales o árboles de decisión. El segundo enfoque corresponde a aquel caso en el que a priori no se conocen los grupos y lo que precisamente se desea es establecerlos a partir de los datos que poseemos. Las técnicas estadísticas más utilizadas en esa área se conocen con el término **análisis cluster**, que podemos traducir como

⁴² Su calibración mediante métodos de machine learning se apoya en técnicas de Bootstrap Aggregating o Bagging (se entrenan los modelos en paralelo y se utiliza la combinación de las predicciones como predicción final) o Boosting (se entrenan los modelos secuencialmente de tal manera que el siguiente modelo se concentre en predecir correctamente los fallos de los anteriores). Ver Breiman, Leo (1996). Bagging predictors 24 (2), o también Dietterich, T. G. (2000, June). Ensemble methods in machine learning. In International workshop on multiple classifier systems. Springer Berlin Heidelberg.



análisis de agrupaciones y también como análisis de conglomerados.

Para ello se pueden comparar distintos modelos, entre los que destacan (ordenados de menor a mayor nivel de sofisticación):

- ▶ **Árbol de decisión:** calibrado de un árbol automático de decisión seleccionando las variables con mayor poder predictivo según el test de “Chi cuadrado” o “Cramer” (la aplicación de cada criterio da lugar a un árbol diferente).
- ▶ **Regresión logística:** selección de un subconjunto de variables con mayor poder predictivo (según el test de “Chi cuadrado”) y calibrado de una regresión logística.
- ▶ **Red Neuronal:** entrenamiento de una red neuronal con las variables originales de la base de entrenamiento.
- ▶ **Transformación + Red Neuronal:** combinación de transformaciones simples (logaritmos, inversas, raíces, potencias, traslaciones, etc.) de variables continuas con las variables originales para el entrenamiento de una red neuronal.
- ▶ **Regresión + Red Neuronal:** combinación de regresión logística para la agregación de variables con una red neuronal.
- ▶ **Random Forest:** combinación secuencial de árboles predictores que dan lugar al llamado “bosque”, que proporcionará una predicción del evento encadenando las predicciones de todos los árboles del proceso.
- ▶ **Gradient Boosting:** combinación de árboles predictores para obtener un clasificador más robusto mediante la aplicación de algoritmos de *machine learning*.

Validación

Con el fin de identificar los modelos que mejor explican el comportamiento de los clientes fraudulentos se fijan algunos criterios mínimos que deben cumplir los resultados obtenidos por el modelo seleccionado.

Estos criterios se basan tanto en la **capacidad discriminante del modelo**, p. ej. su índice AUC⁴³, como en su **razonabilidad**. Esto último se cuantifica mediante el análisis de tendencias (que corrobora que la tendencia del estimador de cada variable, con relación al fraude, se corresponde con lo esperado en términos económicos) y los pesos relativos de las variables según su contribución esperada.

Se ha realizado un ejercicio cuantitativo, ejecutando los modelos descritos en el punto anterior de forma independiente sobre la misma base de entrenamiento. A continuación se muestra una comparativa de su capacidad discriminante en función del área bajo la curva ROC (AUC):

Modelo	ROC sobre base de validación
Árbol de decisión	0.78
Regresión logística	0.74
Red Neuronal	0.82
Transformación + Red Neuronal	0.83
Regresión + Red Neuronal	0.79
Random Forest	0.81
Gradient Boosting	0.86

⁴³ AUC: Area Under the Curve. La curva que se utiliza es la ROC (Receiving Operating Characteristics), que se obtiene a través del porcentaje de individuos bien ordenados por el modelo en función de su propensión al hurto. Es decir, si un modelo identifica a un potencial hurtador con una propensión mayor a otro, la probabilidad de que esto sea correcto se corresponde con el AUC.

Como se puede observar en el análisis realizado, el modelo de **Gradient Boosting** presenta un mayor ajuste en términos de ROC.

Adicionalmente a la validación estadística, se han validado los modelos con las inspecciones realizadas durante seis meses. Se comparan los 12, 25 y 50 clientes con mayor propensión de cada uno de los modelos con las inspecciones realizadas durante ese tiempo para calcular la efectividad de los clientes hurtadores que se obtendría. La siguiente tabla muestra los porcentajes de hurtadores que el modelo encontraría en cada uno de estos grupos (de 12, 25 o 50 clientes).

Modelo	12 clientes	25 clientes	50 clientes
Árbol de decisión	58%	40%	30%
Regresión logística	50%	52%	44%
Red Neuronal	75%	64%	38%
Transformación + Red Neuronal	75%	68%	46%
Regresión + Red Neuronal	67%	60%	42%
Random Forest	75%	64%	52%
Gradient Boosting	92%	72%	50%

Se observa que, sea cual sea el número de inspecciones, el modelo de **Gradient Boosting** es el que recoge una mayor concentración de hurtadores (excepto el **Random Forest** al proponer 50 inspecciones; si bien la mejora no es significativa, un 2%). Por tanto, este modelo es el que se utilizará en el ejemplo práctico.

Ganancia de energía

La ganancia de energía es el concepto usado para representar el **valor económico que se recupera en cada cliente tras la identificación del fraude energético**. Este concepto se corresponde con el valor económico de energía que comienza a



facturarse por la normalización en el consumo tras realizar la inspección más la recuperación de la energía histórica no facturada. Sería el concepto análogo al *Customer Lifetime Value* o valor del cliente usado en las técnicas de segmentación comercial. Su cálculo es una combinación de criterios de negocio definidos por cada compañía, si bien vamos a presentar los principales factores que se consideran para su cálculo:

- **Legislación del país:** la normativa de cada país establece un criterio de penalización por el fraude energético y cómo se debe proceder. A modo ilustrativo, puede consistir en la interrupción del servicio de forma inmediata y en una sanción por el delito basada en una estimación del consumo correspondiente al producto de la potencia contratada, o que se hubiese debido contratar, del suministro donde se produjo la defraudación, por una cantidad de horas de utilización diarias durante un año.
- **Metodología de la estimación del consumo:** según la información que proporciona el medidor, el tipo de contrato, los ciclos de facturación y el histórico de consumo usado, pueden aplicarse criterios diferentes para cada cliente.

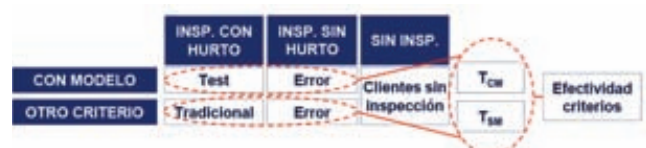
Medición de la efectividad

Las áreas de gestión de la pérdida no técnica de las compañías energéticas invierten recursos humanos, técnicos y económicos en la ejecución de inspecciones a clientes.

La rentabilidad de estas inversiones viene determinada por i) las tasas de éxito observadas (del subconjunto de los clientes inspeccionados, qué porcentaje de clientes con hurto de energía se identificó), ii) la ganancia de energía (representada como valor económico de recuperación por cliente), iii) el número de clientes inspeccionados de la población objetivo, y iv) el coste unitario asociado a la inspección del cliente y por tanto el coste total de la campaña.

Ahora bien, comparar la efectividad de una campaña de inspección determinada por un modelo con otra definida mediante otros criterios de negocio (p. ej. denuncia de los operarios de la manutención o lectura, etc.) requiere de condiciones similares en ambas poblaciones. Es decir, la propensión estructural al hurto en ambas poblaciones debe ser muy similar (p. ej. no se deben comparar zonas de diferente nivel socioeconómico).

El comportamiento de estos modelos se supervisa mediante un seguimiento estadístico del poder predictivo de cada una de las variables usadas y la verificación de su calidad, estabilidad poblacional y capacidad discriminante.



Aplicación práctica

Según se ha indicado en el apartado de validación, se ha seleccionado el algoritmo de mayor poder discriminante. Con este modelo, a continuación se desarrolla un ejemplo de aplicación práctica en la configuración de campañas de inspección.

El ejercicio se enmarca en una distribuidora de electricidad con 5 millones de clientes, donde las **pérdidas no técnicas** representan un 10%. El equipo de pérdidas tiene el objetivo de reducir las pérdidas no técnicas mediante unas **inspecciones** que tienen un coste unitario de 30 USD. Por restricciones operativas y económicas se dispone de 100.000 inspecciones anuales (sensiblemente por debajo del número de clientes hurtadores, que sería del orden de 500.000).

Hasta el momento se ha utilizado un criterio de priorización basado en el **juicio experto del equipo de pérdidas**, que prioriza la inspección de consumos próximos a 0, alcanzando unas tasas de éxito históricas en las inspecciones del 9% (nivel de acierto esperado para campañas realizadas al azar).

El área de pérdidas comienza el desarrollo de un modelo discriminante con la identificación de toda la información histórica disponible de los clientes en un periodo anterior a las inspecciones realizadas. Según se ha expuesto en el apartado de *Fraude interno: segregación de funciones en el ciclo comercial*, se realiza una homogenización de las diferentes fuentes de datos, una selección de información de calidad, la construcción de variables derivadas mediante reglas de negocio y se desarrolla la metodología de selección del modelo.

El modelo seleccionado está basado en árboles de decisión combinados con técnicas de *machine learning*; en concreto, redes neuronales para *deep learning*, apoyándose en variables principalmente de i) **patrón de consumo** –históricos y medias móviles recientes, inspecciones previas-, ii) **características técnicas del punto de suministro** –contadores, acometidas, etc.- y iii) **comportamiento** –reincidencia y otras vinculadas con el recobro, como capacidad y voluntad de pago, etc.-. Este último grupo de variables es especialmente relevante debido a la **vinculación existente entre el hurto y la morosidad**. En general, se trata de dos problemas íntimamente relacionados, dado que en ocasiones la resolución de un problema de hurto da lugar a un problema de impago, y viceversa. Es decir, la falta de capacidad o voluntad de pago deriva en impagos que, cuando son gestionados, por ejemplo a través del corte de suministro, generan un incentivo al hurto. Igualmente, la resolución de un problema de hurto puede generar un problema de impago.

Este modelo **incrementa la tasa de éxito de las inspecciones hasta un 27%** (más de una de cada cuatro inspecciones son exitosas). La siguiente tabla recoge la rentabilidad de las actuaciones antes y después de la implantación del modelo.

Parámetro	Antes... (campaña juicio experto)	Después... (campaña con modelo)
Coste por inspección	30 usd/inspección	30 usd/inspección
Capacidad	100.000 inspecciones/año	100.000 inspecciones/año
Ganancia media de energía	300 usd/hurto	300 usd/hurto
Tasa de éxito	9%	27%
Coste campaña	3.000.000 usd	3.000.000 usd
Ingreso campaña	2.700.000 usd	8.100.000 usd
Resultado campaña	-300.000 usd	5.100.000 usd
Rentabilidad	-10%	170%

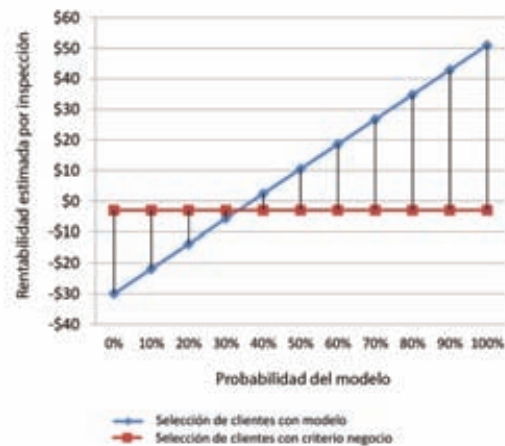
En resumen, el hecho de triplicar la tasa de éxito en las inspecciones y seleccionar el punto correcto de corte para hacer las mismas **incrementa la rentabilidad de las campañas y genera unos beneficios de más de 5 millones de USD para la compañía**, simplemente por el hecho de definir unas campañas de inspección con técnicas de priorización de las visitas basadas en un modelo analítico de propensión al hurto.

La rentabilidad estimada de cada inspección, se define como:

$$\text{Rentabilidad por inspección} \approx \text{Tasa de éxito} * 300 - 30 \frac{\text{USD}}{\text{inspección}}$$

Por ejemplo, el envío de inspecciones a todos los clientes con **una tasa de éxito esperada superior al 50% proporcionaría una rentabilidad esperada por inspección positiva y siempre superior a la rentabilidad mínima exigida (10 USD)**.

Fig.14. Impacto en la rentabilidad de las inspecciones



Conclusiones



Tras exponer el concepto de fraude, externo e interno, y sus implicaciones en términos de organización, procesos y sistemas, se ha puesto el foco en las técnicas de optimización de la gestión del fraude en el sector energético para los casos de hurto de energía y de fraude en el ciclo comercial.

Entre otras **iniciativas**, las compañías energéticas realizan esfuerzos relevantes para la gestión del fraude mediante:

1. La **perfilación de clientes y la segmentación** que les permita orientar sus actuaciones de inspección o mitigación.
2. La definición e implantación de esquemas de **cuantificación de la utilidad y medición de la rentabilidad** de las actuaciones (p. ej. análisis de la rentabilidad de la adquisición de variables externas de proveedores).

El uso de **nuevas técnicas de modelización y machine learning** en estos procesos puede ser una herramienta eficaz en la detección del fraude, incrementando la tasa de éxito, industrializando el proceso de detección del fraude y reduciendo el coste de inspecciones tradicionales.

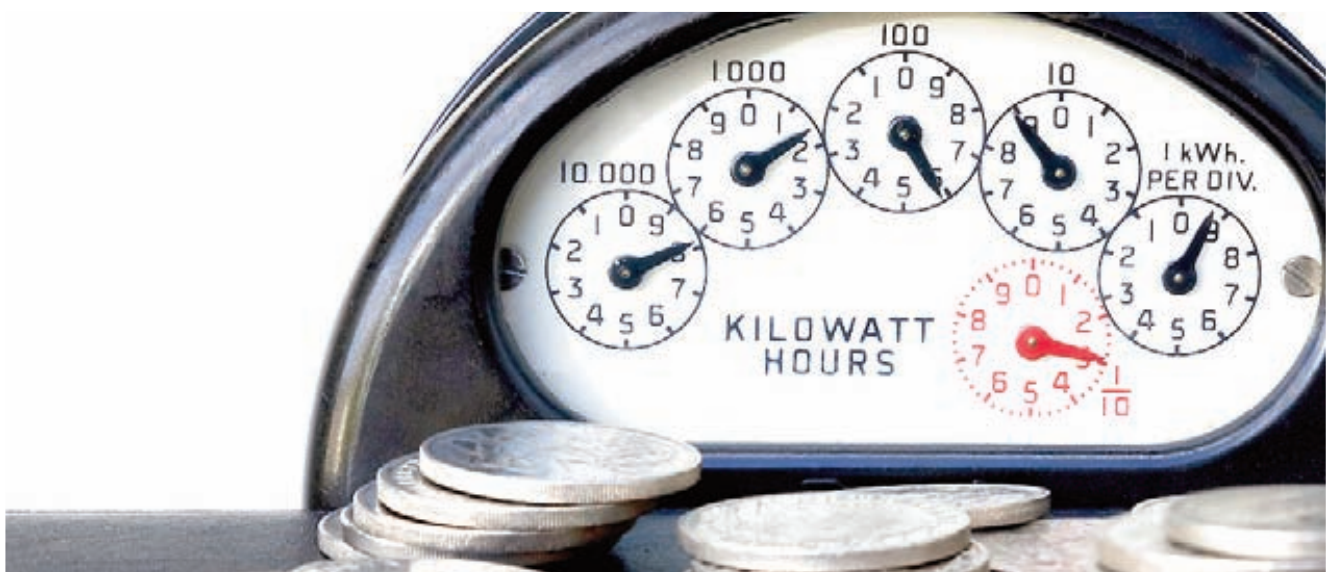
Así, cobra una gran relevancia la **aportación de valor del dato** y de la información de clientes y operaciones en la cuantificación de las posibilidades de ocurrencia de eventos de fraude. La disponibilidad de información (consumos

horarios, datos de clientes, accesos a sistemas, etc.) permite aplicar técnicas tanto de perfilación de clientes y empleados como de segmentación para su gestión personalizada, habiéndose cuantificado ahorros superiores al millón de dólares anuales gracias al análisis de datos en compañías de pequeño tamaño (~2 millones de clientes)⁴⁴. Por ello, se están implantando mecanismos de **gobierno del dato y control de su calidad**.

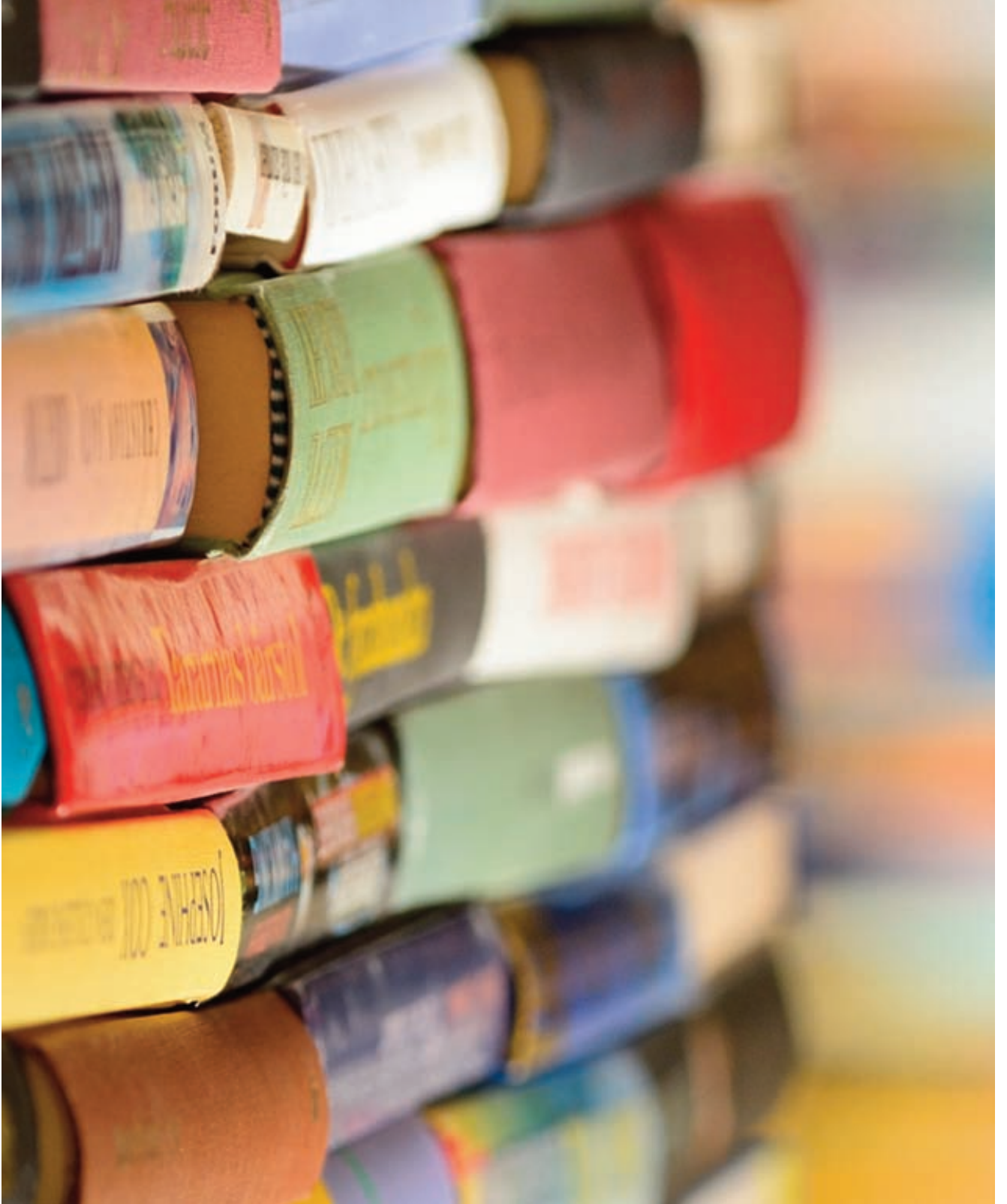
Por otro lado, las actuaciones de detección y mitigación de eventos fraudulentos compiten con el resto de inversiones de la compañía. Por este motivo, su integración en la gestión incorpora la **medición de su rentabilidad**.

Todo ello se engloba en un **marco integral de gestión del fraude**, que puede desarrollarse en las organizaciones para garantizar la consecución de los objetivos de la aplicación de métodos estadísticos.

⁴⁴ Advanced Metering Infrastructure and Customer Systems. Results from the Smart Grid investment grant program. Septiembre 2016, Departamento de Energía de Estados Unidos.



Bibliografía



Report to the nations on occupational fraud and abuse.

Global Fraud Study. ACFE (2016).

Gestión del Riesgo de Fraude en las Organizaciones: una guía práctica.

IIA, Institute of Internal Auditors (2015).

Convergencia internacional de medidas y normas de capital.

Basilea: BCBS (2004).

Other People's Money.

Donald R. Cressey (1973).

Fundamental Elements of Cybersecurity for the financial sector.

G7 Cyber Expert Group (2016).

Reducing Technical and Non-Technical Losses in the Power Sector.

Technical report. World Bank (2009).

Ley 24/2013 del Sector Eléctrico.

Data Science y la transformación del sector financiero.

Management Solutions (2015).

Model Risk Management. Aspectos cuantitativos y cualitativos de la gestión del riesgo de modelo.

Management Solutions (2014).

Managing the Business Risk of Fraud: A Practical Guide.

ACFE (2012).

Game-Theoretic Models of Electricity Theft Detection in Smart Utility Networks: Providing New Capabilities with Advanced Metering Infrastructure.

IEEE Control Systems 35, no. 1 (2015).

Electricity Theft and Non-Technical Losses: Global Markets, Solutions, and Vendors.

Northeast Group, LLC (2017).

Informe sobre las alternativas de regulación en materia de reducción de pérdidas y tratamiento del fraude en el suministro eléctrico.

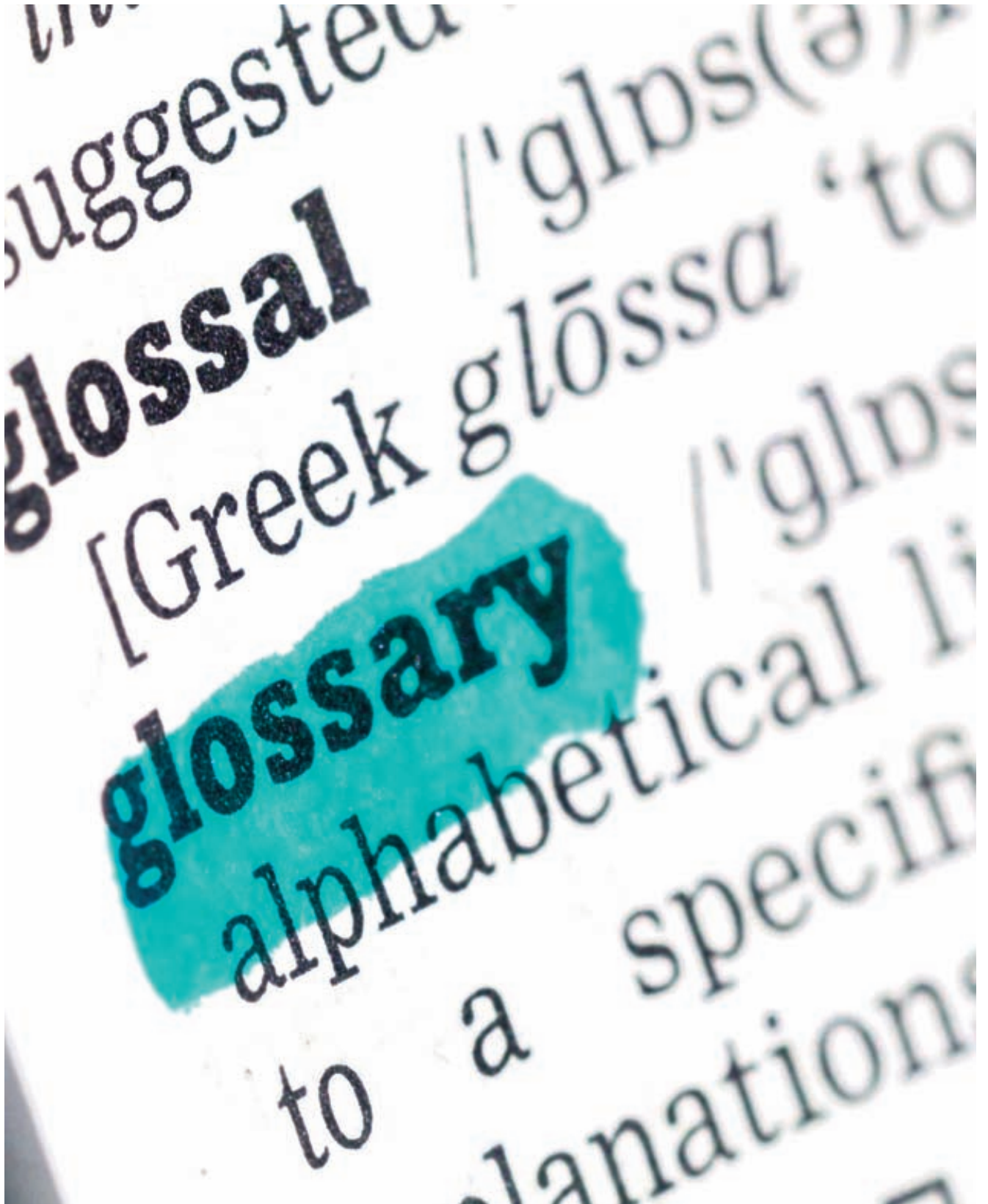
CNMC, Comisión Nacional de los Mercados y la Competencia (Informe de 16 de julio de 2015).

Ley Orgánica de Protección de Datos (LOPD) y a su reglamento de desarrollo (Real Decreto 1720/2007).

Smart Grid investment grant program.

Departamento de Energía de Estados Unidos. (2016).

Glosario



ACFE (Association of Certified Fraud Examiners): establecida en el año 1988, es una organización profesional de examinadores de fraude. Sus actividades consisten en crear herramientas de gestión del fraude, impartir formación y gestionar una base de datos de conocimiento.

AMI (Advanced Metering Infrastructure): sistemas que son capaces de medir, recolectar y analizar el uso de la energía y a su vez interactuar con otros dispositivos como los medidores inteligentes de electricidad, gas o agua. Disponen de la capacidad de gestionar la información recolectada y tomar decisiones. Estos sistemas se diferencian de los sistemas de lectura automática, en que con los AMI existe una comunicación bidireccional entre el medidor y el centro de control de la empresa.

Backtest: término que se refiere al testeo de un modelo predictivo utilizando información histórica para determinar y/o asegurar su rentabilidad.

Chi cuadrado: test estadístico para contrastar la existencia de una relación entre variables.

CFCA (Communications Fraud Control Association): Asociación global de educación sin fines de lucro, que está enfocada a la prevención del fraude en la industria de telecomunicaciones.

COSO (The Committee of Sponsoring Organizations of the Treadway Commission): comité creado a partir de una iniciativa conjunta entre organizaciones pertenecientes al sector privado, dedicado a proveer conocimiento a través del desarrollo de frameworks y guías sobre el control interno, prevención del fraude y gestión del riesgo en las empresas.

Cramer's V: medida de la intensidad de la relación entre dos o más variables categóricas cuando, por lo menos, una de las variables puede tomar al menos dos valores posibles.

Data Lineage: se define como el ciclo de vida de la información que incluye su origen, movimiento y transformaciones. Describe lo que ocurre con la información a medida que se somete a diversos procesos proporcionando visibilidad para poder detectar los errores y sus fuentes.

Deep Learning: conjunto de algoritmos de aprendizaje automático que intentan aprender representaciones de datos. Una observación (por ejemplo, una imagen) puede ser representada de muchas formas (por ejemplo, un vector de píxeles), pero algunas representaciones hacen más fácil aprender tareas de interés (por ejemplo, "¿es esta imagen una cara humana?").

Financial Fraud Action UK: organismo responsable de liderar la lucha colectiva contra el fraude en nombre de la industria financiera del Reino Unido; siendo su función primordial facilitar la actividad entre los diferentes actores involucrados en la lucha contra el fraude.

IIA (Institute of Internal Auditors): asociación internacional profesional de auditoría interna y gestión de riesgos establecida en el año 1941.

KDD (Knowledge Discovery in Database): proceso de extracción de información potencialmente útil de una base de datos. Proceso iterativo que exhaustivamente explora volúmenes muy grandes de datos para determinar relaciones.

KPI (Key Performance Indicator): métrica que utilizan las entidades para medir los resultados de una determinada acción o estrategia en función de unos objetivos predeterminados.

Machine Learning: método de análisis de datos que automatiza el proceso de la creación de modelos analíticos. Utiliza un algoritmo que iterativamente aprende de la información, permitiendo a las herramientas encontrar patrones escondidos sin tener que estar explícitamente programadas para ello.

Minería de datos (Data Mining): proceso computacional para descubrir patrones ocultos, tendencias y correlaciones a través de la extracción de una gran cantidad de datos.

NIST (National Institute of Standards and Technology): agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos cuya misión es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología.

Phishing: intento de obtener información sensible como usuarios, contraseñas, información de tarjetas de crédito, etc., generalmente con intenciones maliciosas, engañando a entidades legítimas mediante una comunicación electrónica.

SM (Smart Meters): equipo electrónico que captura el consumo energético en intervalos de una hora o menos y a su vez comunica la información recolectada al centro de control de la empresa para su monitoreo o facturación de la electricidad.

SoD (Segregation of Duties): concepto de dedicar a más de una persona para realizar una tarea. Es una medida de control que divide una tarea en subprocesos, asignándolos a diferentes responsables, para prevenir fraude.

Stream Computing: sistema informático que analiza múltiples flujos de datos de diversas fuentes, procesando la información, transmitiéndola de vuelta en un solo flujo.



Nuestro objetivo es superar las expectativas de nuestros clientes convirtiéndonos en socios de confianza

Management Solutions es una firma internacional de servicios de consultoría centrada en el asesoramiento de negocio, finanzas, riesgos, organización y procesos, tanto en sus componentes funcionales como en la implantación de sus tecnologías relacionadas.

Con un equipo multidisciplinar (funcionales, matemáticos, técnicos, etc.) de cerca de 2.000 profesionales, Management Solutions desarrolla su actividad a través de 24 oficinas (11 en Europa, 12 en América y 1 en Asia).

Para dar cobertura a las necesidades de sus clientes, Management Solutions tiene estructuradas sus prácticas por industrias (Entidades Financieras, Energía y Telecomunicaciones) y por líneas de actividad (FCRC, RBC, NT) que agrupan una amplia gama de competencias: Estrategia, Gestión Comercial y Marketing, Gestión y Control de Riesgos, Información de Gestión y Financiera, Transformación: Organización y Procesos, y Nuevas Tecnologías.

En la industria de energía, Management Solutions presta servicios a todo tipo de sociedades -eléctricas, gasistas, petroquímicas, etc.- tanto en corporaciones globales como en compañías locales y organismos públicos.

Jesús Martínez

Socio de Management Solutions
jesus.martinez.gimenez@msspain.com

Manuel Ángel Guzmán

Gerente de I+D de Management Solutions
manuel.guzman@msspain.com

Javier Salcedo

Supervisor de Management Solutions
javier.salcedo@msbrazil.com

Diseño y Maquetación
Dpto. Marketing y Comunicación
Management Solutions - España

© **Management Solutions. 2017**
Todos los derechos reservados

www.managementolutions.com

Madrid Barcelona Bilbao London Frankfurt Paris Warszawa Zürich Milano Roma Lisboa Beijing New York Boston Atlanta
Birmingham San Juan de Puerto Rico Ciudad de México Medellín Bogotá São Paulo Lima Santiago de Chile Buenos Aires