PROSEGUR RESEARCH

Crime on business brief

El contexto global del **fraude interno**

2023

PROSEGUR

HOME

ÍNDICE

01

Una importante **amenaza interna**

HOME

01
Una importante amenaza interna

02
El fraude interno en clave analítica

03
Una visión estratégica sobre el fenómeno

04
Tendencias del fraude interno

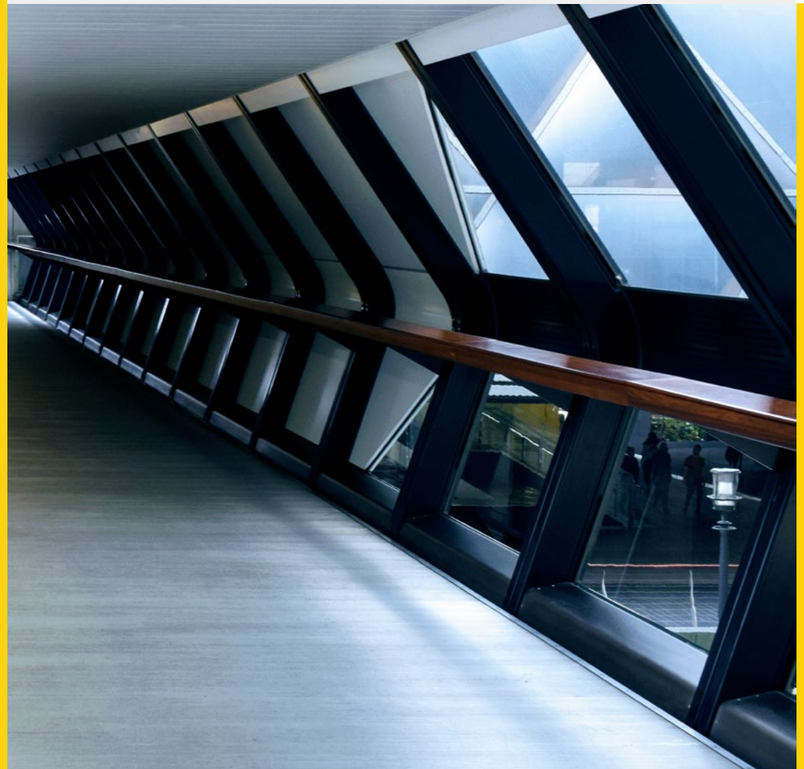
01

UNA IMPORTANTE AMENAZA INTERNA

Las organizaciones públicas y privadas se enfrentan a una serie de desafíos y riesgos para la seguridad y la continuidad de negocio con multitud de aristas e impactos. En este sentido**, el fraude interno se configura como uno de los actos delictivos o ilícitos con mayor impacto** reputacional, social, de gobernanza y económico para las organizaciones.

Así, este informe de Prosegur Research se enmarca dentro de una serie de **estudios** sobre **cultura de seguridad,** que profundiza sobre los fenómenos delictivos que se cometen en el seno de las empresas; en este caso, se analizan las complejas dinámicas y los diversos contextos en los que se acometen los delitos de **fraude en el ámbito corporativo.**

Al enfrentarse a este reto las empresas deben considerar que se trata de un **problema complejo,** para el que **no existe solución conocida ni única,** por lo que se deben emplear todos los recursos adecuados humanos y tecnológicos desde la comprensión del fenómeno y con una visión estratégica que inhiba conductas indeseables en el seno de la empresa y que, en el peor de los casos, minimice su impacto.



Desde Prosegur Research entendemos el fraude interno – en terminología anglosajona *occupational fraud* – como el **acto intencional y deliberado** de los trabajadores de una compañía o de terceras partes con **acceso** a la misma para generar **lucro personal y/o causar otros daños** de diversa índole. Entre las acciones se incluyen la manipulación o falsificación de registros, la malversación de activos, la filtración de datos o todas aquellas acciones que afecten en última instancia a la estabilidad económica, operacional y reputacional como la apropiación indebida.

Las **amenazas internas,** originadas en el seno de la empresa, suponen grandes pérdidas económicas y de información para las entidades víctima de su impacto. Además de generar disrupciones en la actividad económica de la empresa, las consecuencias de dichas amenazas pueden repercutir sobre su imagen y reputación en la opinión pública. No obstante, se deben **diferenciar estos hechos de los fraudes externos,** puesto que éstos se cometen por actores ajenos a una organización. Así, la **normativa ISO/CD 37003,** que se encuentra en estado de desarrollo, establecería que un fraude interno debe involucrar, al menos, a un autor conectado de forma directa a la organización objetivo de fraude.

El fraude en el ámbito corporativo cuenta con una serie de características que lo configuran como problema complejo, ya que generalmente existe una **baja disponibilidad de información sobre su incidencia, lo que dificulta la dimensión y la categorización de las amenazas,** debido a la **infradenuncia** de estos actos por parte de las compañías. Por ejemplo, según IBM, se tarda de media **197 días en detectar una filtración de datos y hasta 77 días en recuperarse** de la misma. Por este motivo, se trata de un fenómeno con una **considerable "cifra negra"** y los datos existentes y publicados en estudios e informes son **escasos y difícilmente comparables entre sí,** basados en estudios de caso, lo que dificulta la creación de planes de prevención y mitigación.

De esta manera, el fraude interno requiere un profundo ejercicio de análisis **cualitativo y reflexión** para poder comprender los **drivers que lo propician,** las **tendencias** y, en la medida de lo posible, **anticiparse a sus impactos y responder en consecuencia.**

En este contexto, uno de los principales actores con mayor potencial impacto sobre las organizaciones es el denominado **insider,** es decir, un miembro de la compañía o un trabajador externo que tiene o ha tenido acceso a la entidad por prestar algún servicio para la misma y lo utiliza para llevar a cabo **voluntaria y conscientemente acciones para obtener un beneficio personal,** usualmente de carácter económico o de venganza y resentimiento hacia la corporación.

HOME

Gráfico 1
El iceberg del fraude interno

Fuente: Prosegur Research, 2023

Ninguna organización, ni por su tamaño, ni por su sector, es ajena a este fenómeno, pudiendo producirse en circunstancias muy diversas y propiciada por factores variados.

En definitiva, no debemos olvidar que a cargo de cada negocio, ya sea desde la oficina, en el comité de dirección o a pie de calle, se encuentra una persona: entender sus motivaciones, y sobre todo sus desmotivaciones, así como el entorno en el que operan a nivel particular y organizacional es lo que nos permitirá generar una **cultura de seguridad** adecuada para erradicar, o al menos detectar y mitigar, este fenómeno tan oculto y sus importantes impactos.

HOME

02

El fraude interno **en clave analítica**

HOME

01 Una importante amenaza interna

02 El fraude interno en clave analítica

03 Una visión estratégica sobre el fenómeno

04 Tendencias del fraude interno

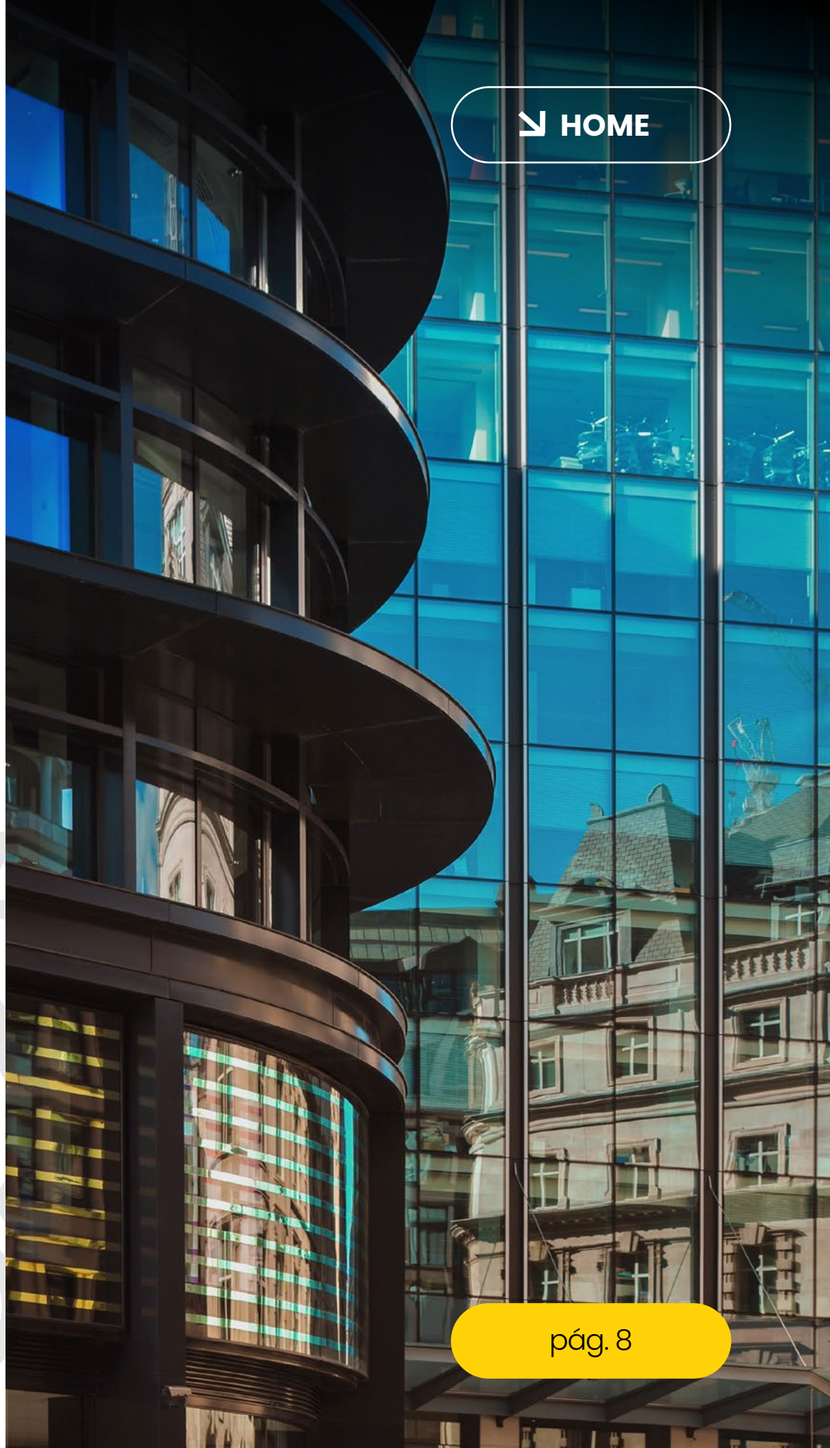
02

EL FRAUDE INTERNO EN CLAVE ANALÍTICA

2.1 Modelos generales explicativos del fraude

El sector al que pertenece la compañía, aun teniendo en cuenta que muchas empresas son multisectoriales, influye fuertemente en el modus operandi e impactos del fraude interno en cada negocio. Por este motivo, **los modelos generales explicativos del fraude interno no se pueden aplicar a todo sector y todo tipo de empresa, por lo que los rasgos característicos del fenómeno hay que buscarlos a través de una reflexión más estratégica.** A modo de ejemplo, las amenazas por fraude en el seno de la empresa a las que se enfrenta el sector bancario, orientadas mayormente a la ingeniería o evasión fiscal, se diferencian en gran medida del sector retail o el sector servicios, orientadas al hurto, la pérdida desconocida o el fraude en la facturación, entre otras.

Además, como se ha venido señalando **los impactos del fraude interno no se limitan únicamente a la pérdida económica,** sino que puede afectar a la reputación, la confianza de los stakeholders, la cotización en bolsa, el acceso a licitaciones o la capacidad de contratar proveedores.



HOME

Atendiendo al conocido ***árbol de fraude*** de la Association of Certified Fraud Examiners (ACFE), existen tres tipologías principales de fraude interno:

Apropiación indebida de activos

Se trata de la dimensión con una relación más directa con la seguridad física, por lo que puede ser el aspecto más visible del fraude interno, puesto que incluye ilícitos como el raterismo, las ventas falsas de stock, el robo de materiales o la creación de facturas falsas para apropiarse de ellos.

- **Raterismo**
- **Ventas falsas de stock**
- **Robo de materiales**
- **Creación de facturas falsas**

Manipulación de información financiera

Se relaciona con los activos financieros, las cuentas fraudulentas y la evasión fiscal, incluyendo actos como la valoración inapropiada de bienes o los ingresos ficticios, entre otros.

- **Valoración inapropiada de bienes**
- **Ingresos ficticios**

Prácticas relacionadas con la corrupción

Incluye todos aquellos actos en los que la corrupción influye de manera directa, tales como la extorsión económica, el soborno, las comisiones o los conflictos de intereses.

- **Extorsión económica**
- **Soborno**
- **Comisiones**
- **Conflictos de intereses**

Fuente: Prosegur Research, 2023 basado en ACFE

Según el último ***Occupational Fraud Report 2022,*** las prácticas relacionadas con la **corrupción** y la **apropiación indebida de activos** son los tipos de fraude **más comunes a nivel global,** siendo además habitual su concurrencia. Al respecto, no hay sector sin fraude, puesto que cualquier compañía puede ser víctima de estos delitos.

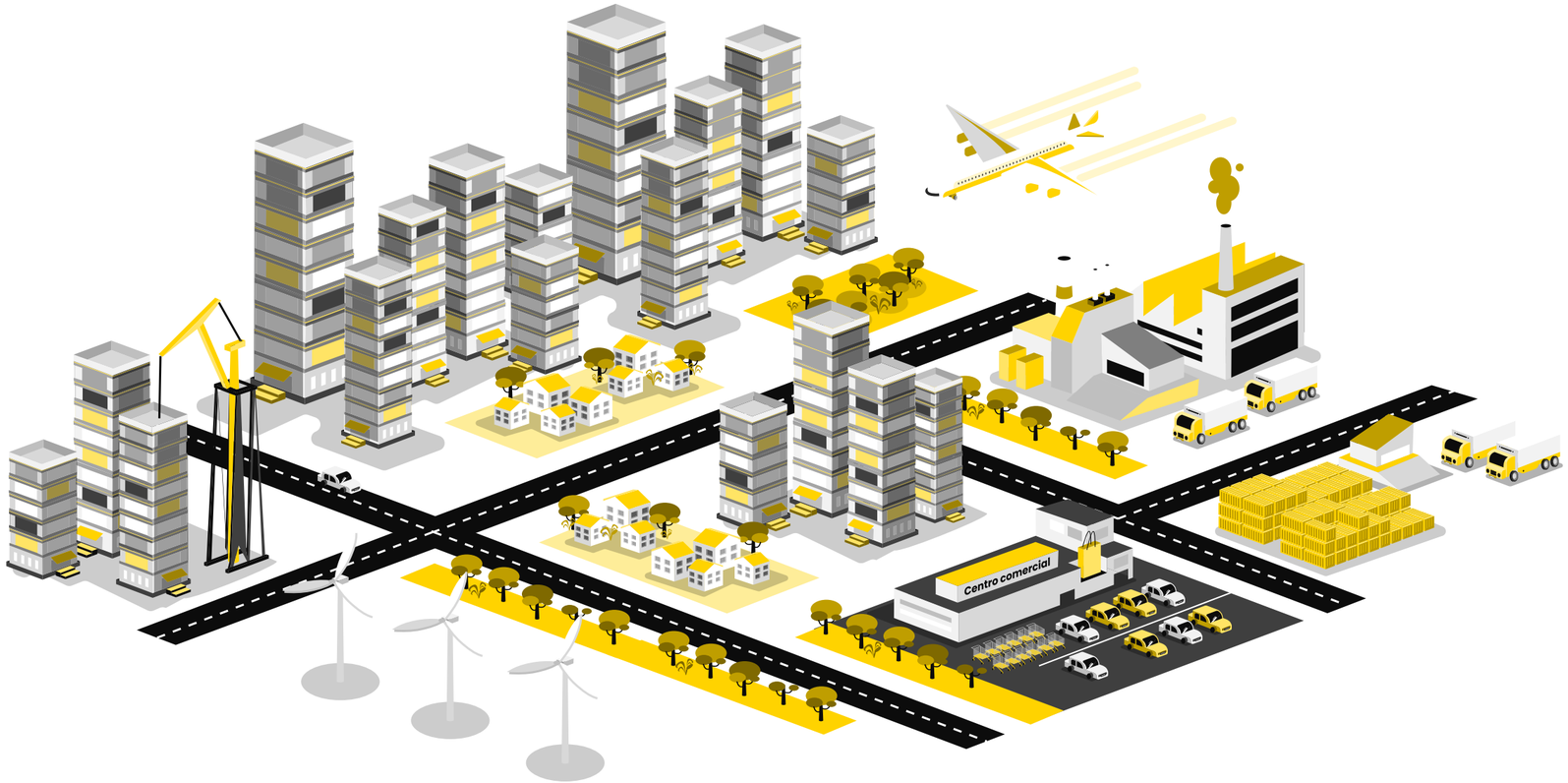
Abordar la explicación y las motivaciones de una persona para cometer un fraude interno resulta complejo. A lo largo de las últimas décadas se ha intentado explicar este fenómeno, pensando en el conocimiento necesario para poder enfrentarlo con garantías y rigurosidad. Entre los **principales modelos explicativos** destacan el triángulo del fraude y el diamante del fraude, expuestos a continuación.

Gráfico 2
No hay sector sin fraude

Fuente: Prosegur Research, 2023

HOME

Bancas y finanzas | Industria | Transporte | Logística



Real Estate | Energía | Retail | Tecnología

HOME

Por una parte, el **triángulo del fraude** se basa en un modelo propuesto por Cressey en 1972 basado en ***tres componentes fundamentales para cometer un fraude interno:***

Oportunidad
Para llevar a cabo una de estas acciones se deben producir diferentes circunstancias, como la posibilidad de hacerlo o la ausencia de controles, lo que facilita la perpetración del acto delictivo.

Presión financiera
También denominado "motivación", se refiere a la razón por la que se comete el fraude, generalmente de orden económico.

Racionalización
El trabajador que comete un fraude interno trata de justificar o autoconvencerse de que dicho acto está justificado, relacionándose con aspectos emocionales y subjetivos como la ira hacia la empresa, la aparente impunidad o la percepción de un salario inadecuado.

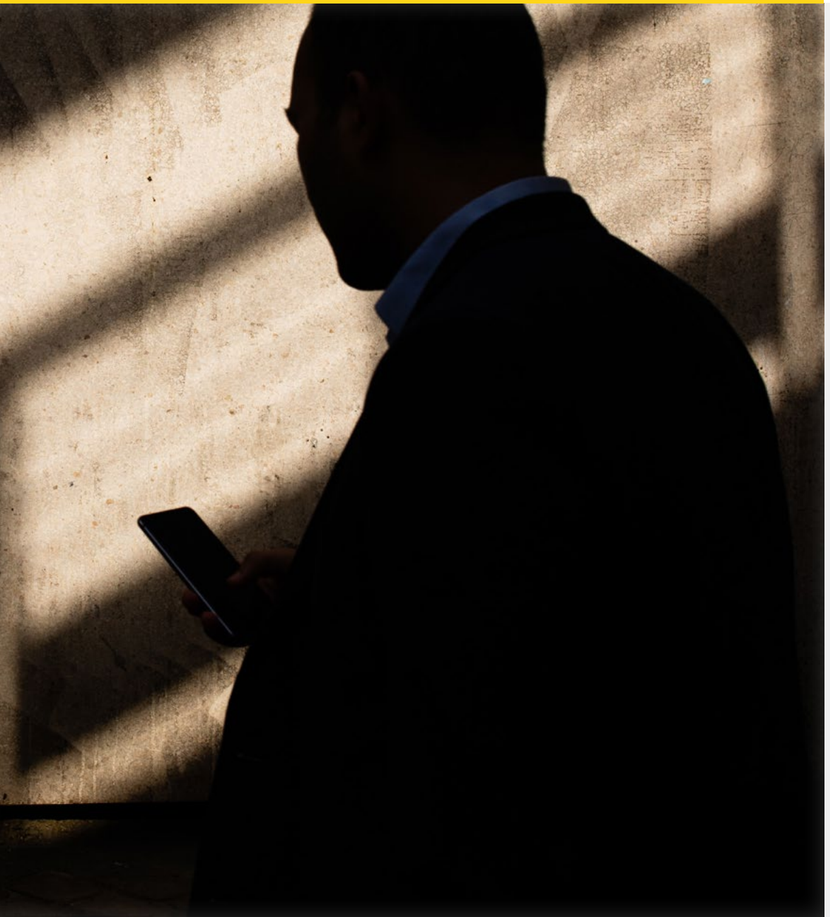
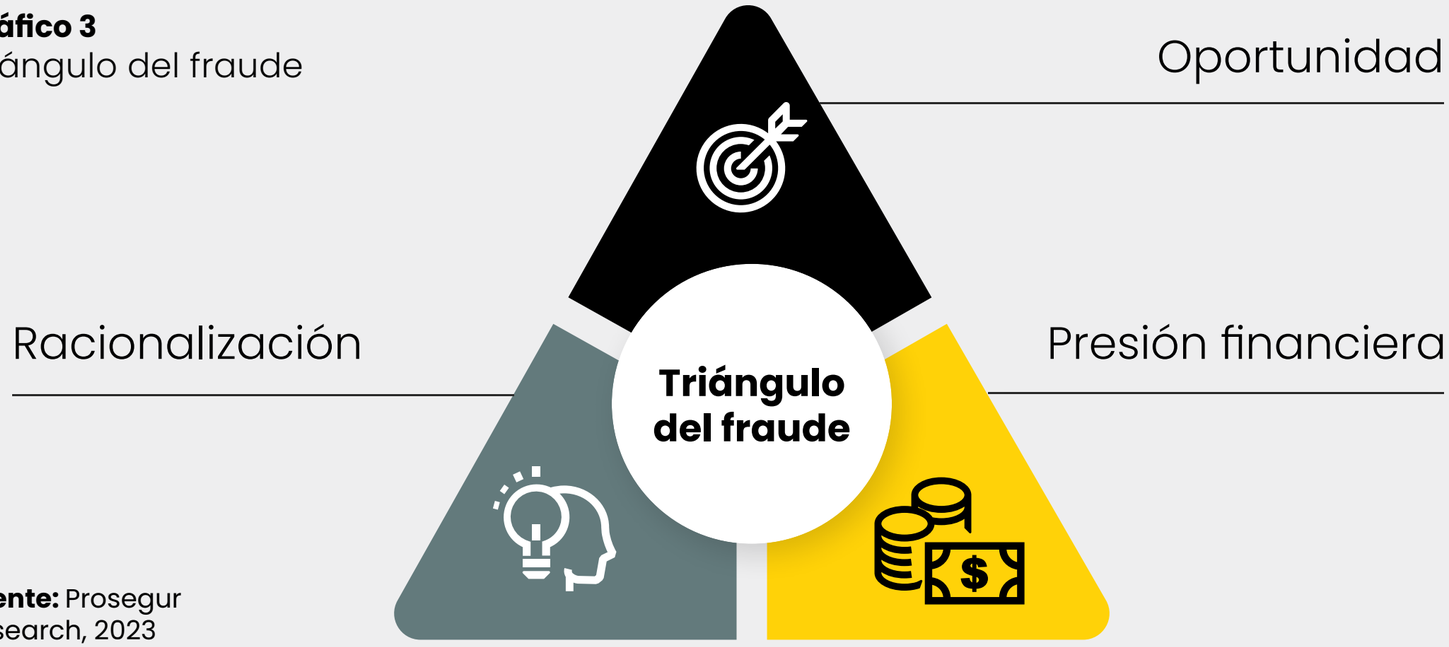
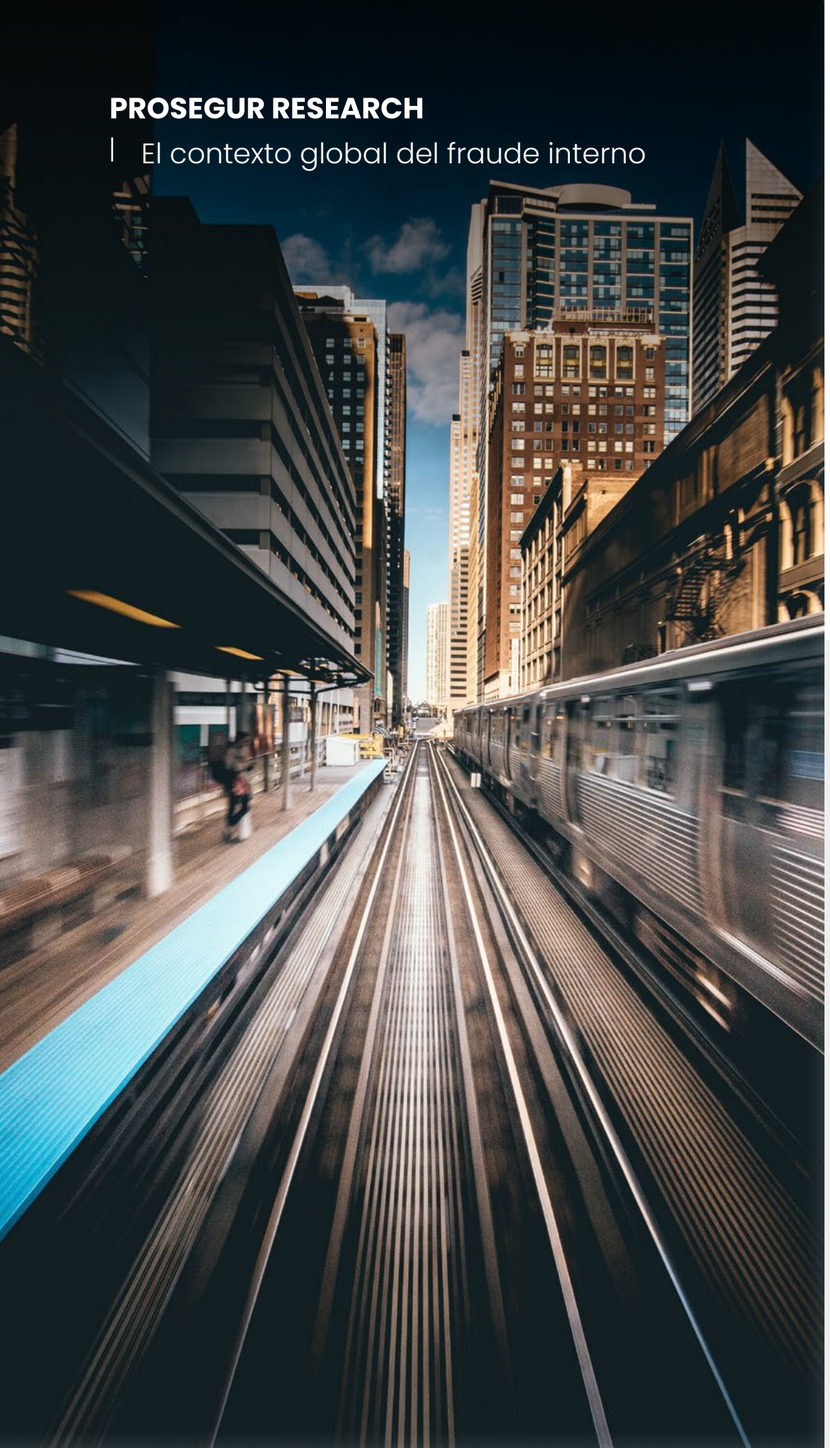


Gráfico 3
Triángulo del fraude



Fuente: Prosegur Research, 2023



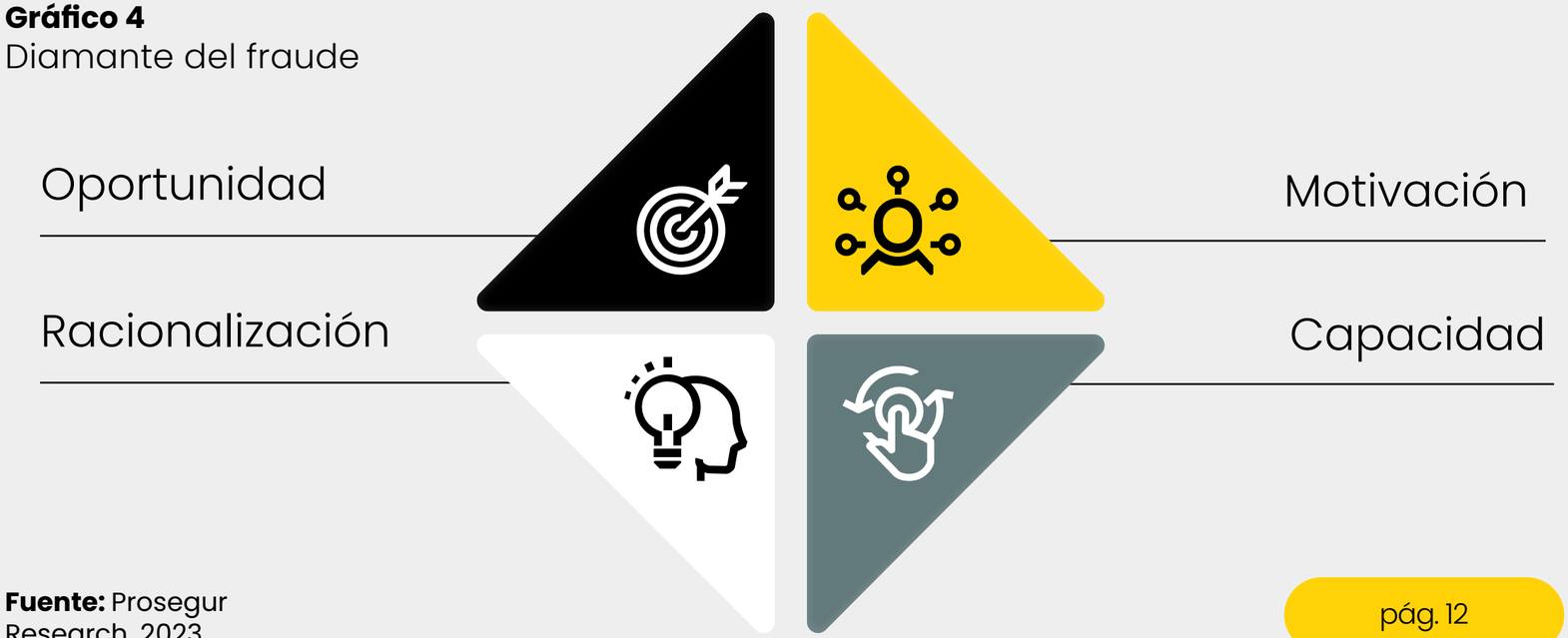
HOME

Algunas críticas hacia este modelo han derivado en la creación del conocido **"diamante del fraude",** el cual, además de los tres elementos anteriores, incluye una cuarta arista: la **capacidad** para llevar a cabo el fraude interno, es decir, la disposición de conocimiento y recursos para ello. Adicionalmente, la presión financiera se amplía a un abanico más amplio de motivaciones e incentivos.

La **ausencia o debilidad de controles internos, la falta de dirección y supervisión,** el **deseo de beneficio económico,** las **dificultades personales** o la sensación de estar **infravalorado** en la empresa son algunos de los principales factores que propician el fraude interno en las organizaciones, según han señalado algunos estudios, como por ejemplo los realizados por **KPMG.**

Asimismo, desde la World Compliance Association (WCA) se ha argumentado que otros factores como la **rotación de puestos** de trabajo, la **no segregación** de funciones o los **bajos salarios** pueden llevar a una persona descontenta con su trabajo a cometer un fraude interno.

Gráfico 4
Diamante del fraude



Fuente: Prosegur Research, 2023

HOME

2.2 La visión de Prosegur Research sobre el fraude interno

Desde el punto de vista de Prosegur Research, el análisis del contexto, una **inteligencia contextual,** es preciso para completar la visión sobre el fraude interno, dado que no es un fenómeno que exclusivamente se produce como decisión de un empleado al margen de todo un contexto bastante más amplio y mucho más dinámico, como lo son las tendencias globales y las dinámicas internas empresariales. Así, todo fenómeno delictivo se desarrolla en un **contexto temporal y espacial** determinado, pero siempre es susceptible de ser afectado por **multitud de variables** contextuales políticas, sociales, económicas o tecnológicas.

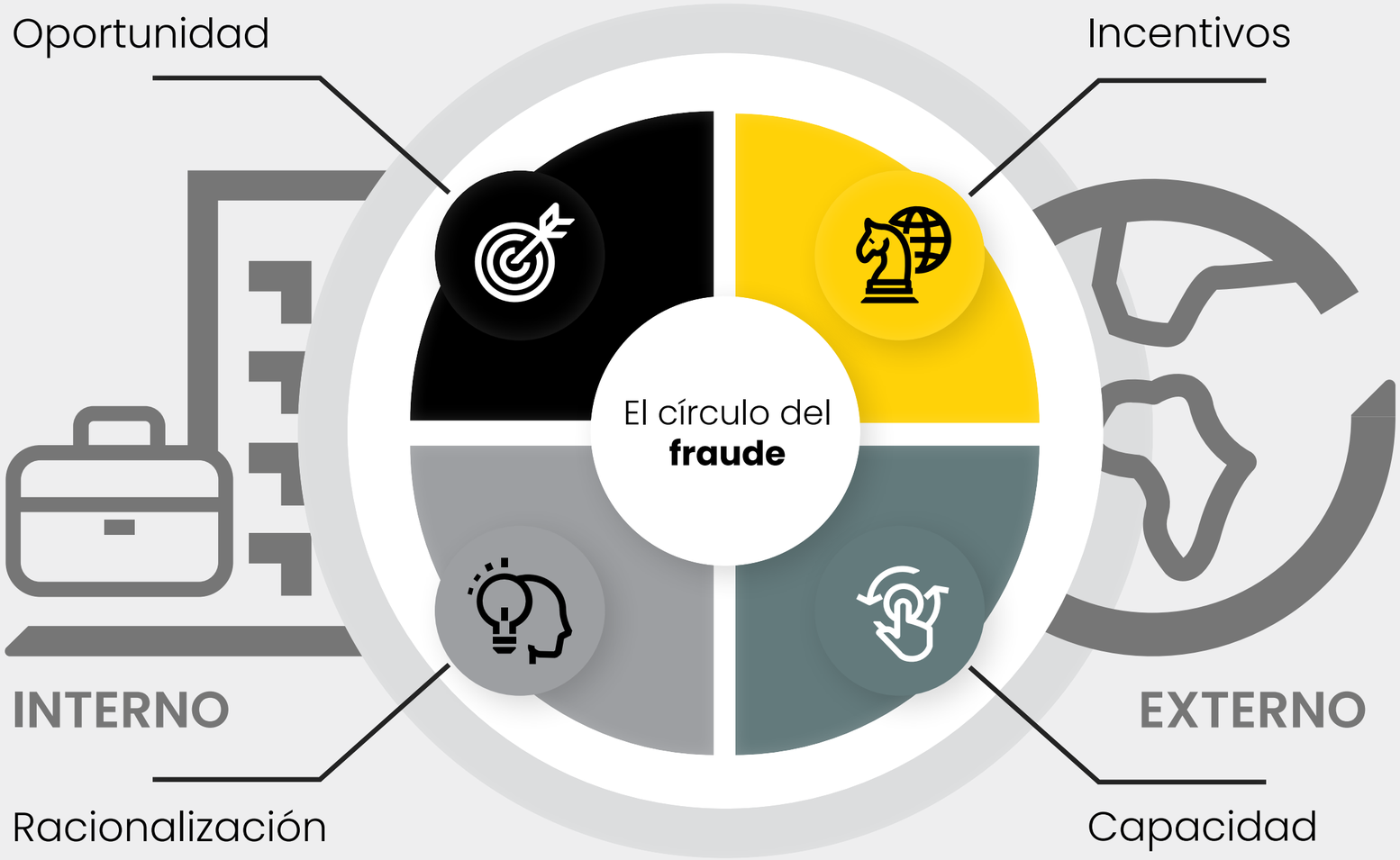
Actualmente el mundo se caracteriza por lo que está siendo denominado **permacrisis,** un largo periodo de inestabilidad e inseguridad, especialmente tras la pandemia de COVID-19 y el conflicto de Ucrania, o **policrisis,** según los últimos informes del Foro Económico Mundial sobre **riesgos globales.** En este contexto, se precisa realizar una reflexión profunda sobre las principales variables que están afectando al mundo en su presente y futuro, además de los **efectos sistémicos** que la interacción entre diferentes tipologías de riesgos genera, amplificando en muchos casos sus impactos.

La lucha contra el fraude interno es una **labor integral y transversal en las organizaciones,** ya que puede afectar a diferentes departamentos. Por ello es importante tener claridad en la estructura sobre las responsabilidades de cada una de las áreas involucradas porque en caso contrario se puede producir una gestión caótica y conflictiva con duplicidades, invasión de competencias o problemas de liderazgo, entre otros.

HOME

Gráfico 5
El círculo del fraude

Fuente: Prosegur Research, 2023



Así pues, **la explicación del fraude interno no se puede separar del análisis del contexto externo global e interno empresarial,** además de contar con las cuatro variables principales que motivan a una persona a cometer este hecho delictivo: oportunidad, incentivo o motivación, capacidad y racionalización.

Por tanto, la crisis económica, el cambio social, el **empoderamiento individual,** los cambios de modelos de trabajo hacia formatos híbridos o el **desarrollo tecnológico** generan impactos trascendentales en fenómenos delictivos como puede ser el fraude interno o riesgo del insider, afectando especialmente a las motivaciones y objetivos perseguidos por sus autores, así como al modus operandi en que se desarrollan.

Así, **desde Prosegur Research se propone un modelo de fraude interno** atendiendo a las variables externas e internas que pueden impactar en este fenómeno:

A **Longitud de miras:** el impacto del contexto externo

Las sociedades y consecuentemente la economía, las políticas y las tecnologías evolucionan de una forma acelerada, impactando a cualquier fenómeno vinculado a la seguridad. De esta manera, **la inseguridad es, en gran medida, una situación contextual.**

El trabajador de una compañía, independientemente de si es pública o privada, **no es ajeno ante los cambios del ambiente,** por lo que las variables externas pueden influir de una manera determinante sobre su comportamiento:

1 Inestabilidad económica o financiera

Las subidas de tipos de interés, la inflación, la caída del poder adquisitivo, los costes de la vivienda o la inestabilidad laboral son algunas de las variables que pueden actuar como incentivo para el defraudador.

2 Corrupción

Una elevada percepción de corrupción y la aparente normalización a todos los niveles de la sociedad potencia la racionalización del hecho delictivo.

3 Incertidumbre

La percepción del riesgo constante por los ciudadanos se enmarca en el contexto actual caracterizado por la fragilidad, la ansiedad, la incomprensibilidad y la no linealidad de los hechos – tal y como expone el paradigma BANI – tras algunos riesgos sistémicos observados en los últimos años, como la guerra en Ucrania o la pandemia de COVID-19, lo que potencia un estado de ansiedad constante tanto colectivo como individual.

4 Complejidad

La tecnificación (el desarrollo de las nuevas tecnologías y la transformación digital) y la complejidad financiera privilegia a los actores que cuentan con las capacidades para llevar a cabo un fraude interno, aumentado a su vez el criterio de oportunidad.

5 Anomia

La ausencia de sentimiento de pertenencia a la organización, la falta de confianza en las autoridades e instituciones y la aparente impunidad reincide en la justificación de los hechos.

6 Individualismo

Uno de los mayores retos para las empresas en la actualidad es la retención del talento, con empleados con una exigencia creciente en sus condiciones laborales, como se ha observado en los últimos meses en la adopción del teletrabajo, por ejemplo. Los ciudadanos, en general, y los trabajadores, en particular, se caracterizan por la exigencia y una progresiva pérdida de lealtad tradicional hacia las compañías.

7 Era de las contradicciones

El mayor acceso al conocimiento y recursos actualmente, en gran medida propiciados por Internet, aumenta el criterio de capacidad para el fraude, pudiendo realizar en solitario acciones que hace años resultaban impensables.

B

Profundidad de miras: la cultura de empresa como elemento diferenciador

En el contexto interno se deben tener en consideración aquellas cuestiones que están afectando de forma dinámica y con elevada volatilidad a las organizaciones empresariales y que pueden **modular el fenómeno del fraude,** facilitando, potenciando y produciendo sinergias entre contexto interno, externo y el individual.

Así, son igualmente variados los factores que se deben analizar en cada compañía:

1

Transformación digital

Las capacidades de la automatización de tareas y procesos conllevan importantes beneficios para los trabajadores y las empresas, si bien en ocasiones se producen brechas de edad digitales, que, unido a los problemas de las plataformas de gestión tecnológicas, pueden suponer frustraciones para el empleado.

2

Dimensión internacional de las organizaciones

La confluencia de diferentes culturas empresariales y de seguridad, con hábitos y formas de gestión diferentes, puede implicar en ocasiones la normalización de algunas acciones fraudulentas en otros países.

3

Inestabilidad

La inestabilidad presente en la práctica totalidad de compañías ante el desarrollo tecnológico, la evolución del sector, los ajustes continuos de personal o la viabilidad futura de la empresa son algunas de las variables que pueden actuar como incentivos para el defraudador.

4

Carácter multisectorial

Las actividades transversales en diferentes sectores de las corporaciones aumentan potencialmente las formas de realización de fraudes, lo que amplía los vectores de ataque en el seno de la empresa.

5

Evolución de las áreas de seguridad y riesgos

La seguridad es un concepto evolutivo y cambiante y los departamentos de seguridad no siempre evolucionan a la misma velocidad que los cambios de los fenómenos delictivos, uniéndose además a los pocos recursos disponibles para los mismos y la ausencia de la especialización que requiere el fraude interno.

6

Modelos reactivos vs. estratégicos

En ocasiones los planes contra el fraude interno con los que cuentan las corporaciones tienen un carácter eminentemente reactivo, siendo necesaria la creación de planes de prevención y anticipación ante estos hechos desde la madurez de modelos estratégicos.

03

Una visión estratégica sobre el fenómeno

HOME

01 Una importante amenaza interna

02 El fraude interno en clave analítica

03 Una visión estratégica sobre el fenómeno

04 Tendencias del fraude interno

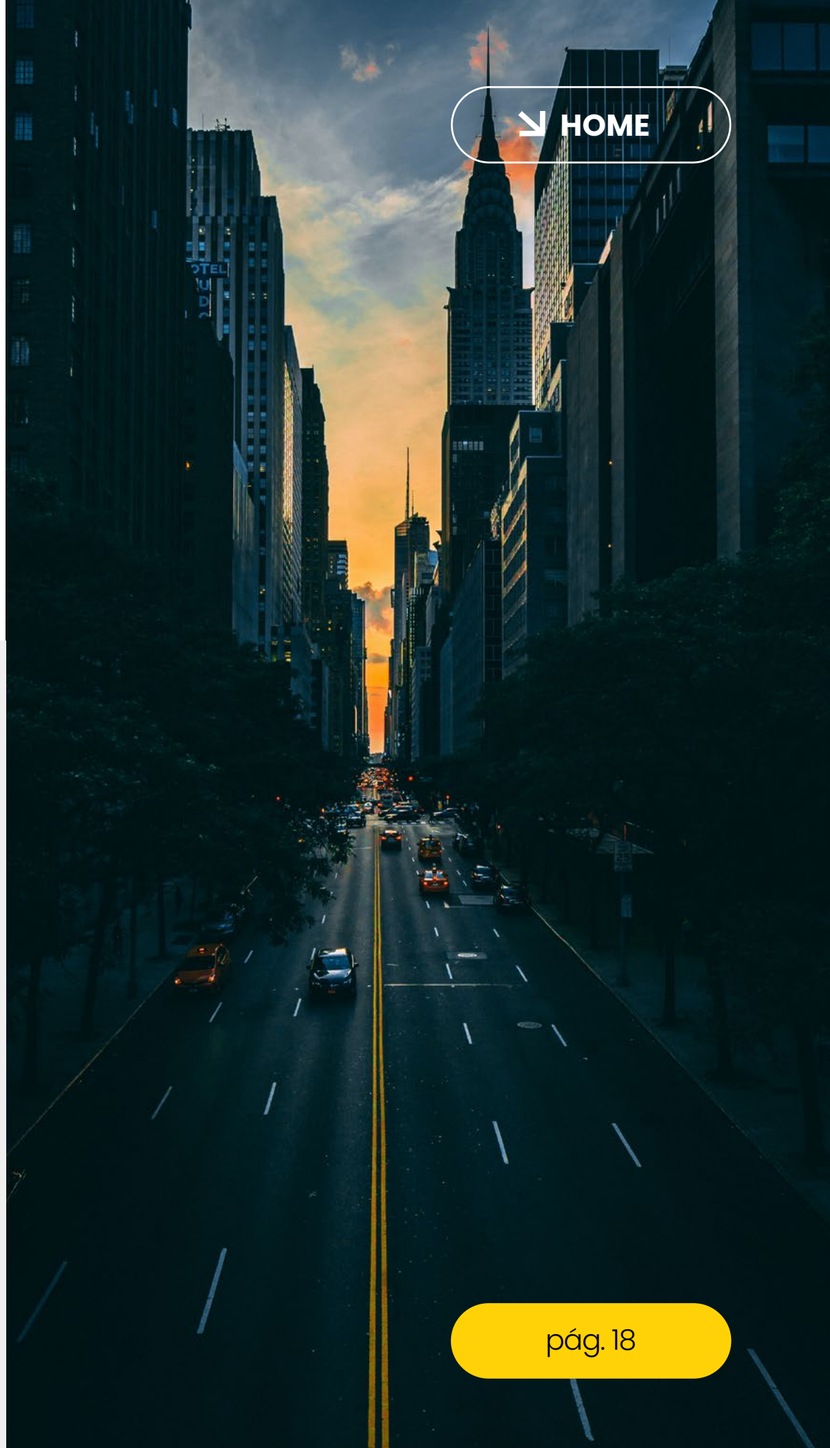
03 UNA VISIÓN ESTRATÉGICA SOBRE EL FENÓMENO

3.1 Una estructura organizativa clara

Atendiendo al marco de análisis expuesto con anterioridad, se debe concebir a cada **organización como un sistema holístico** para crear **programas estructurales** contra el fraude interno. Por este motivo, la **acción empresarial** debe orientarse hacia la **estrategia** y la creación de planes de prevención y reacción eficaces, para lo cual la **inteligencia** es uno de los principales activos con los que cuenta cualquier compañía.

Gráfico 6
La pirámide de la acción empresarial

Fuente: Prosegur Research, 2023



HOME

HOME

El **fraude interno,** una vez que se produce, afecta a todo el ecosistema corporativo, viéndose afectados multitud de departamentos directa o indirectamente relacionados entre sí. Desde la inmediata respuesta que deben dar los **equipos de recursos humanos, gestión de riesgos y cumplimiento,** todos aquellos relacionados con la **comunicación** deben minimizar su impacto y trasladar a todos los stakeholders relacionados de manera eficaz el mensaje adecuado.

Además, se deben potenciar y mejorar los canales de **seguridad y las tecnologías de la información,** de manera que en última instancia se reduzca su impacto en áreas de relevancia organizacional como la **financiera** o las **ventas**, garantizando en última instancia la continuidad de negocio y la operatividad de toda la organización.

Todo ello deriva en la **cultura de empresa** como un elemento diferenciador para evitar la perpetración del fraude interno. Es parte de las responsabilidades de la organización velar por el correcto desempeño del empleado y, en la medida de lo posible, de su bienestar, debiendo incidir en la supervisión y en los criterios ambientales, sociales y de gobernanza (ESG) para acentuar el **propósito** de la compañía e incrementar el **engagement** del trabajador. Al respecto, las compañías que cuentan con unas políticas ESG fuertes y visibles cuentan con un ***14% más de satisfacción del trabajador.***

Gráfico 7
El fraude interno en el ecosistema corporativo

Fuente: Prosegur Research, 2023

3.2 **Análisis** de riesgos

El análisis de riesgos es el proceso para identificar, analizar y evaluar los riesgos de fraude interno con objeto de adoptar las medidas necesarias para su eliminación o, al menos, mitigación.

Tras el análisis del contexto interno y externo mediante **herramientas y procesos pormenorizados y metódicos,** en el que se incluyen algunas como el PESTEL, el DAFO o el análisis de datos, se identifican los riesgos y las áreas críticas donde puede producirse el fraude en el ámbito corporativo. Así, **se determinan las fuentes de las amenazas y las vulnerabilidades,** asignando probabilidad, impacto y exposición, para finalmente **proponer y adoptar las medidas** que resulten necesarias.

Gráfico 8
Gestión del riesgo del fraude interno

Fuente: Prosegur Research, 2023

HOME

A Prevención

La **prevención** es el principal objetivo de una estrategia contra el fraude interno, creando un contexto para que el fraude no se produzca y actuando consecuentemente para disminuir la variable de oportunidad en el modelo del fraude interno, sin descartar impactos derivados en los incentivos, la capacidad y la racionalización.

Es por este motivo que los planes para la **prevención del fraude** y las técnicas de compliance resultan de gran relevancia para las empresas. Según la WCA, **hasta el 80% de las empresas de múltiples sectores reconocen haber sido víctima de fraude** y, sin embargo, más de la mitad no cuenta con sistemas integrales de prevención, a pesar de que **el 85% de los empleados que cometen estos actos muestran señales de riesgo.**

Por tanto, resultan de interés tanto las **medidas de carácter más estático,** como los códigos de conducta, el canal de denuncias o la difusión de una cultura de cumplimiento, **como las de carácter práctico,** con la implementación de controles, auditorías, monitorización y KPIs.

HOME

B Detección

La detección es el segundo objetivo de las estrategias contra el fraude, si bien se caracteriza por ser una **acción de alta complejidad,** dada la relación de confianza en la que se basa la prestación laboral y la involucración de multitud de variables interconectadas.

Uno de los aspectos de mayor relevancia para la lucha contra el fraude interno en el momento de la **detección** son las **señales de riesgo,** o **"red flags",** que pueden mostrar los trabajadores, incluyendo **factores personales, organizacionales y otros estresores** como una presión excesiva, una elevada irritabilidad, la presencia de problemas de índole personal, el incumplimiento de políticas de compliance o la complejidad de procesos y sistemas organizativos.

Según la ACFE, entre las vías más habituales para la detección del fraude destaca la **denuncia** como la más habitual. Así, la presencia de **canales éticos y de comunicación bidireccional** entre el empleado y la compañía, así como la realización de **background checks** e informes de idoneidad de personal y directivos para la detección de señales son algunas de las herramientas que pueden ayudar a las organizaciones a reducir el impacto del fraude interno.

C Respuesta

Una vez detectado un caso, o ante su sospecha, y siempre bajo el amparo normativo preciso en cada región geográfica, se requiere dar una **respuesta integral,** con el objetivo de demostrar el ilícito, establecer la responsabilidad por el mismo y obtener la evidencia suficiente y necesaria para poder actuar disciplinaria y/o judicialmente.

Esta respuesta integral debe darse a todos los niveles. Por una parte, la **investigación** sobre el mismo debe ser conducida por equipos altamente especializados que cuenten con fundamentos forenses en relación a cuentas financieras, análisis documental, forense digital, análisis de inteligencia y trabajo de campo. Adicionalmente, tras la recogida de **evidencias** se deben llevar a la práctica las acciones que se consideren necesarias, entre las que se encuentran el régimen disciplinario, la desvinculación con la organización o las acciones legales oportunas. Por último, no se puede dejar de lado el proceso de análisis para extraer **insights sobre las lecciones aprendidas** y ajustar los controles existentes y la cultura empresarial para reducir las posibilidades de perpetración de este acto.

A Prevención

Acciones estáticas

- Política empresarial
- Códigos de conducta
- Formación
- Concienciación
- Canal de denuncias

Acciones prácticas

- Auditorías
- Controles
- Monitorización
- Alertas
- KPIS

B Detección

Los defraudadores suelen mostrar **un comportamiento sospechoso previo**

- Factores personales
- Factores organizacionales
- Estresores
- Comportamientos

C Respuesta

Investigación

- Análisis forense
- Inteligencia contra el fraude
- Trabajo de campo

Evidencias

- Régimen disciplinario
- Desvinculación
- Acciones legales

Otras acciones

- Comunicación
- Lecciones aprendidas
- Ajuste de controles

HOME

01
Una importante amenaza interna

02
El fraude interno en clave analítica

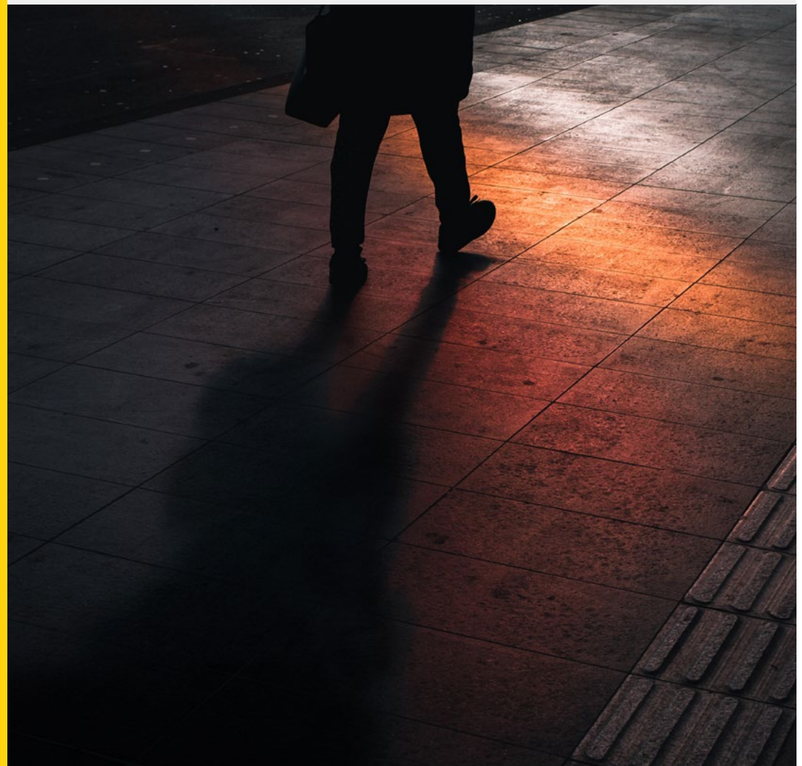
03
Una visión estratégica sobre el fenómeno

04
Tendencias del fraude interno

04

Tendencias del fraude interno

04 TENDENCIAS DEL FRAUDE INTERNO



Como se ha dejado patente a lo largo del documento, el fraude interno es un **fenómeno complejo, evolutivo** y en el que la innovación también juega un papel importante. Por tanto, su abordamiento desde las organizaciones lejos de ser una tarea burocrática debe realizarse también con mentalidad abierta y estratégica.

Así, las **tendencias en los desarrollos tecnológicos** están suponiendo un auge en **nuevas formas de fraude** que las empresas deben tener en cuenta a la hora de desarrollar sus planes de prevención y mitigación: por ejemplo, **hasta el 8% de todos los casos de fraude detectados en 2022 se relacionaron con criptomonedas,** originalmente no diseñadas para el fraude pero que en la actualidad ayuda a cometer sobornos y apropiaciones indebidas de activos. Tal y como señala la ACFE, **es previsible un aumento en los próximos años en la comisión de fraudes internos relacionados con criptomonedas,** especialmente si se consolida la tendencia en su uso por parte de las compañías y la sociedad. Por este motivo es fundamental contar con planes de prevención fórmulas de investigación y medidas reactivas adecuadas desde el apoyo de organizaciones con solvencia y experiencia en este ámbito.

Adicionalmente, las **plataformas** han ganado una gran relevancia en la operatividad de los negocios a nivel mundial en los últimos años, incluyendo plataformas financieras, empresariales, redes sociales y comunicación, etc. En este sentido, PwC señala una **nueva modalidad delictiva en la delincuencia económica,** conocida como **fraudes de plataforma.** Atendiendo a los datos ofrecidos por la compañía, **el 91% de las organizaciones analizadas han experimentado en los últimos 24 meses este tipo de actividad criminal.** Asimismo, en más de la mitad de los casos estos fraudes conllevan pérdidas económicas, con otro tipo de consecuencias adicionales como el daño a la cultura organizacional y a la reputación. Además, **en el 51% de los casos estos hechos se llevan a cabo por fuentes internas o por una confluencia de amenazas internas y externas, con una relevancia creciente del crimen organizado.**

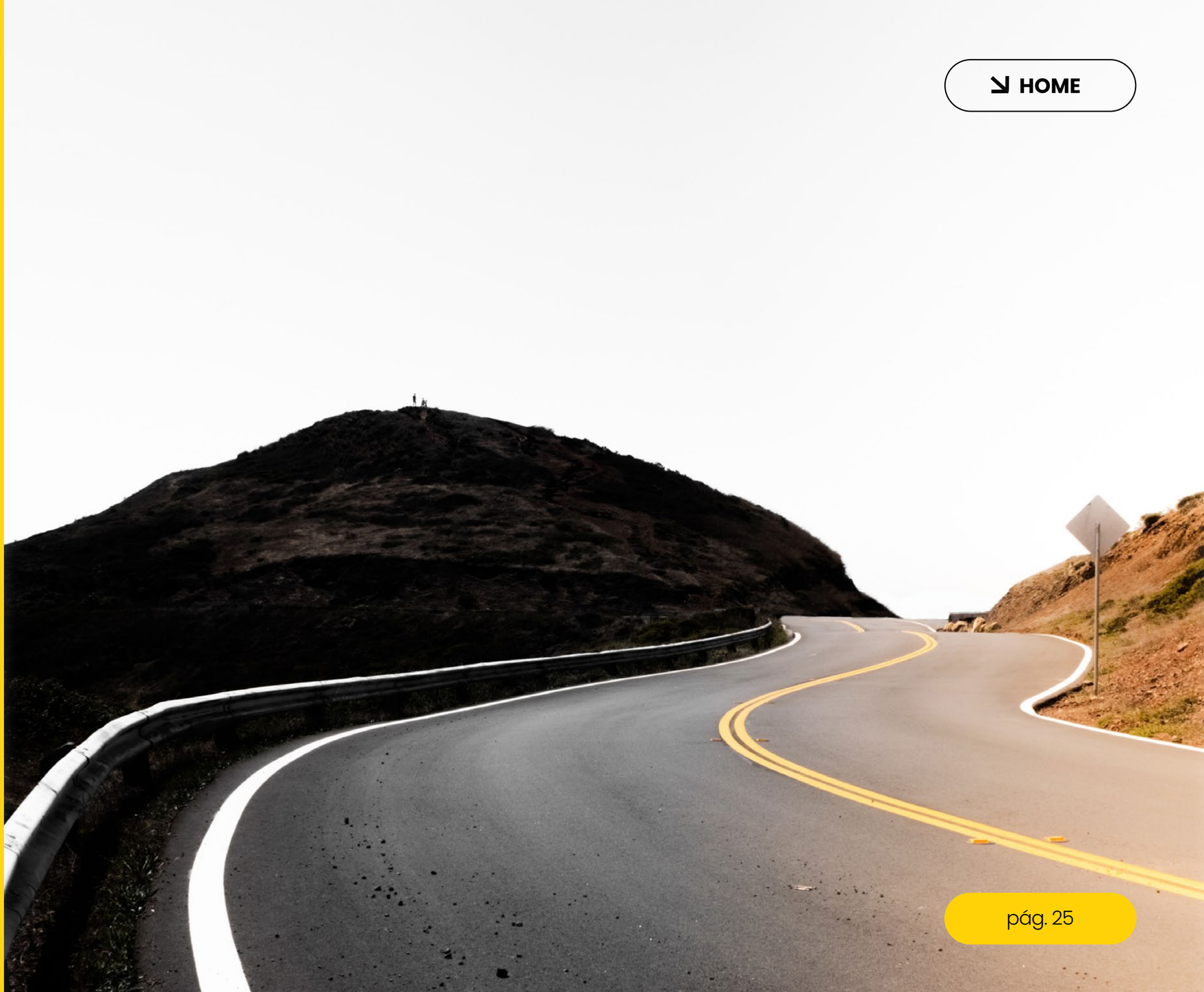
Por otra parte, el **fraude del CEO,** también conocido como Business Email Compromise (BEC) en terminología anglosajona, es **una de las líneas delictivas con mayor aumento en los últimos años,** tal y como señala el **Internet Crime Report 2021** del FBI, propiciado por la adopción del **teletrabajo,** llegando a registrarse casos en más de 150 países de todo el mundo. Así, los **ciberataques** han experimentado un aumento exponencial, de hasta el **125% en 2021** tras la pandemia de COVID-19. Es por este motivo que los delincuentes tratan de ganar acceso en la compañía utilizando a empleados de la misma, normalmente del C-Suit, haciéndose pasar por el CEO. Al respecto, si bien no se configura inicialmente como un fraude interno, se hace necesaria la acción de un empleado, en ocasiones por desconocimiento o negligencia, para poder perpetrarse, por lo que la **combinación de fuentes internas y externas** en este ámbito es crucial. De esta manera, es previsible que continúen en incremento en los próximos

HOME

años los ataques de **phishing, ingeniería social y otros derivados como el spear phishing o el executive whaling** dependiendo del objetivo de ataque.

La progresiva adopción en un número cada vez mayor de ámbitos de nuestra vida de aparatos y sistemas tecnológicos está dificultando los planes de prevención de fraudes de multitud de compañías. Según señalan Forbes y Experian, la **suplantación de identidades** potenciada por la inteligencia artificial y los **deepfakes** conocida como ***"Frankenstein IDs",*** bien sea por actores internos o externos a la organización, dificulta la **prevención basada en biometría,** por lo que la ciberseguridad jugará un papel crucial en la continuidad de negocio en los próximos años.

Por último, más allá de los variados impactos de la tecnología en esta materia, no se debe obviar el **contexto sociopolítico y económico** en el que el empleado se encuentra inmerso. Variables como las **dificultades económicas,** las altas **tasas inflacionarias** en multitud de Estados como Venezuela, Argentina, Zimbabue o Turquía, entre otros, o la elevada conflictividad social pueden **potenciar el riesgo de fraude interno, especialmente si las condiciones desfavorables se mantienen en los próximos meses,** disminuyendo el poder adquisitivo y la calidad de vida de los ciudadanos.



HOME

Todas estas tendencias tienen la finalidad de situar el fenómeno en un contexto futuro, pero sin duda creemos que ese futuro será positivo; para ello desde Prosegur Research añadimos tres **elementos clave de la cultura corporativa para inhibir conductas fraudulentas:**

A Las personas con criterio marcan la diferencia

Las empresas realizan duros esfuerzos en captación y retención del talento, lo que en realidad incluye contar con **empleados con criterio** que realicen su labor diligentemente, pero **más allá del papel**[1]**:** sabiendo qué hacer cuando el protocolo no se ajusta a la compleja y cambiante realidad, generando valor desde la innovación sensata contra ensoñaciones y venta ambulante de humo e impregnando la oficina con autenticidad y vitalidad en aras de la consolidación del negocio.

[1] Lo que el antropólogo Hutchins ya en 1995 llamaba **Cognition in the Wild** (Cognición en estado natural) en sus estudios sobre las complejidades de navegación a las que se enfrentaban las tripulaciones de la Armada estadounidense, analizando las disposiciones en el trabajo cognitivo en estas situaciones a diferencia del típico estudio de laboratorio.

B Confianza en toda la cadena de valor

En toda actividad empresarial, la **solvencia es una verdadera ventaja competitiva;** erradicar conductas fraudulentas pasa por generar una arquitectura de compromiso desde la compañía, que permita el crecimiento profesional y personal de los empleados. Para ello, en la era de la inmediatez inundada de KPIs, debemos **desburocratizar desde la confianza en el empleado,** y generar espacios para las nuevas formas de trabajo, de liderazgo, de aprendizaje y, en definitiva, de vida.

C Contra el trabajo en silos: generosidad

Pocas situaciones son tan paralizantes en una empresa como la departamentalización de tareas y la compartimentalización de objetivos; una empresa transparente debe fomentar el **pensamiento sistémico y las conductas altruistas** en su día a día. No se trata de filantropía ni esplendidez, más bien de entrenar la empatía de esos empleados sensatos y confiables para **orientar los esfuerzos hacia el propósito común.**

Y es que una empresa sin propósito atrae empleados sin misión ni valores; por ello, generar comunidad de trabajo incluyendo el criterio, la confianza y la generosidad como parte del clima laboral permite superar la arrogancia de "lo mío" y **construir un futuro positivo desde "lo nuestro".** Esta idea no consiste en forzar a los empleados a priorizar la empresa frente a sus propios intereses, más bien en alinear los objetivos de cada uno hacia los intereses de ambos dentro del propósito, de forma que sea un *win-win.* **Priorizar nuestro lado más humano** es la mejor forma de inhibir conductas indeseables y promover la cultura de seguridad desde la naturaleza de **los buenos empleados, que los datos nos dicen que son la mayoría.**

PROSEGUR

Garantizamos la seguridad de las personas,
las empresas y la sociedad en su conjunto.

research@prosegur.com

PROSEGUR **RESEARCH**

www.prosegurresearch.com