



**Jorge Badillo**



**Tema:**

**Sistema de alertas para la detección de riesgos de fraude: proactividad, innovación y tecnología.**





# Sistema de alertas para la detección de riesgos de fraude

Jorge Badillo  
Junio – 2025

# Jorge Badillo Ayala

- ▶ Es ecuatoriano, cuenta con más de 26 años de experiencia en labores de auditoría: interna, financiera, de gestión, forense, informática. Trabaja en la compañía SCM Minera Lumina Copper Chile (Joint Venture: Lundin Mining – Canadá & JXNMM – Japón) como Gerente de Auditoría Interna.
- ▶ Tiempo atrás trabajó en la compañía minera Sierra Gorda SCM (Joint Venture: KGHM – Polonia & Sumitomo – Japón) como Gerente de Auditoría Interna con sede en Chile, también trabajó en la compañía minera canadiense Kinross Gold Corporation como Gerente Regional de Auditoría Interna para Sudamérica, con sede regional en Chile. Trabajó para la Organización de las Naciones Unidas ONU como Contralor Financiero de la Organización Internacional para las Migraciones, Misión en Ecuador; antes se desempeñó en Ecuador como Manager en Ernst & Young y también fue Director de Auditoría Interna del Servicio de Rentas Internas – SRI.
- ▶ Es Doctor en Contabilidad y Auditoría - CPA; Magíster en Administración de Empresas – MBA; Diplomado en Control de Gestión; Diplomado en Gestión en la Minería; Diplomado en Compliance Corporativo.
- ▶ Cuenta con las certificaciones/calificaciones internacionales:
  - ▶ CIA – Certified Internal Auditor
  - ▶ QIAL – Qualification in Internal Audit Leadership
  - ▶ CCSA – Certification in Control Self – Assessment
  - ▶ CGAP – Certified Government Auditing Professional
  - ▶ CRMA – Certification in Risk Management Assurance
  - ▶ CISA – Certified Information Systems Auditor
  - ▶ CFE – Certified Fraud Examiner
- ▶ Es miembro del Directorio en The Institute of Internal Auditors (The IIA Global). Es miembro de Comités Internacionales en The IIA (2008 – 2024).
- ▶ Fue Presidente de la Fundación Latinoamericana de Auditores Internos – FLAI. Fue Presidente del Instituto de Auditores Internos del Ecuador. También fue miembro del Directorio del Instituto de Auditores Internos de Chile.
- ▶ A nivel internacional es conferencista, instructor y docente universitario en los temas de su especialidad.



**Jorge Badillo**



# Contenido

---

1. Gestión del Riesgo de Fraude (GRF)
2. Tecnología aplicada a la GRF
3. Sistema de alertas para la detección de riesgos de fraude
4. Conclusión

# 1. Gestión del riesgo de fraude



# 1. Gestión del riesgo de fraude



# 1. Gestión del riesgo de fraude

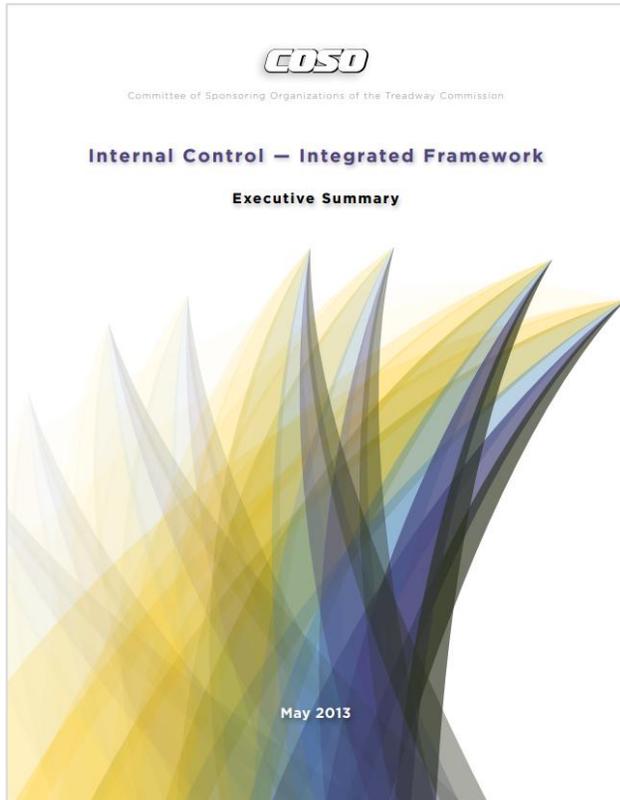
---



# 1. Gestión del riesgo de fraude



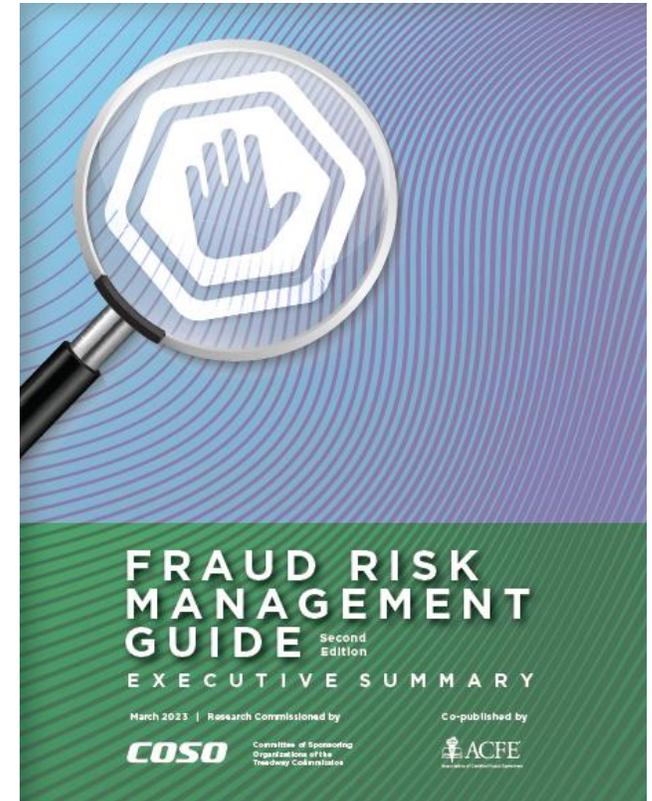
## Comité COSO



**COSO – Control Interno**  
2da edición – 2013  
1ra edición – 1992



**COSO – Gestión de Riesgos**  
2da edición – 2017  
1ra edición – 2004



**COSO – Gestión de Riesgo de Fraude**  
2da edición – 2023  
1ra edición – 2016

# 1. Gestión del riesgo de fraude

## Actualización de COSO Gestión de Riesgos de Fraude



Fuente:  
<https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/fraud-risk-management-guide>

# Guía de Gestión de Riesgo de Fraude – COSO (2023)

## Summary of Fraud Risk Management Components and Principles

### Fraud Risk Governance

Fraud risk governance is an integral component of corporate governance and the internal control environment. Corporate governance addresses the manner in which the board of directors and management meet their respective obligations to achieve the organization's goals, including its fiduciary,

reporting, and legal responsibilities to stakeholders. The internal control environment creates the discipline that supports the assessment of risks to the achievement of the organization's goals.



Control Environment

### Principle 1

The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.

### Fraud Risk Assessments

A fraud risk assessment is a dynamic and iterative process for identifying and assessing fraud risks relevant to the organization. Fraud risk assessment addresses the risk of fraudulent financial reporting, fraudulent non-financial reporting, asset misappropriation, and corruption (including illegal acts and noncompliance with laws and regulations).

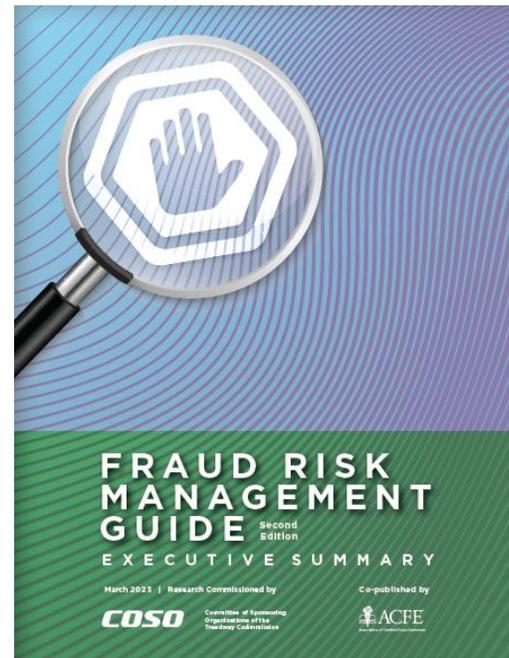
Organizations can tailor this approach to meet their individual needs, complexities, and goals. Fraud risk assessment is not only an integral component of risk assessment and internal control, it also is specifically linked to COSO 2013 IC Framework Principle 8.



Risk Assessment

### Principle 2

The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.



### Fraud Control Activity

A fraud control activity is an action established through policies and procedures that helps ensure that management's directives to mitigate fraud risks are carried out. A fraud control activity is a specific procedure or process intended either to prevent fraud from occurring or to detect fraud quickly in the event that it occurs.

Fraud control activities are generally classified as either preventive (designed to avoid a fraudulent event or transaction at the time of initial occurrence) or detective (designed to discover a fraudulent event or transaction

after the initial processing has occurred). The selection, development, implementation, and monitoring of fraud preventive and fraud detective control activities are crucial elements of managing fraud risk. Fraud control activities are documented with descriptions of the identified fraud risk and scheme, the fraud control activity that is designed to mitigate the fraud risk, and the identification of those responsible for the fraud control activity. Fraud control activities are integral to the ongoing fraud risk assessment component of internal control.



Control Activities

### Principle 3

The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.

### Fraud Investigation and Corrective Action

Control activities cannot provide absolute assurance against fraud. As a result, the organization's governing board ensures that the organization develops and implements a system for prompt, competent, and confidential review, investigation, and resolution of instances of

allegations involving potential fraud and misconduct. An organization can improve its chances of loss recovery, while minimizing exposure to litigation and damage to reputation, by establishing and carefully preplanning investigation and corrective action processes.



Information & Communication

### Principle 4

The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

### Fraud Risk Management Monitoring Activities

The fifth fraud risk management principle relates to monitoring the overall Fraud Risk Management Program. Organizations use fraud risk management monitoring activities to ensure that each of the five principles of fraud risk management is present and functioning as designed and that the organization identifies needed changes in a timely manner.

the fraud monitoring activities. Similar to the COSO 2013 IC Framework, ongoing evaluations in a Fraud Risk Management Program that are built into the organization's business processes at varying levels provide timely information. In contrast, organizations conduct separate evaluations periodically that vary in scope and timing based on numerous factors, including the results of ongoing evaluations.

Organizations use ongoing and separate (periodic) evaluations, or some combination of the two, to perform



Monitoring Activities

### Principle 5

The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.

Fuente:

<https://www.acfe.com/fraud-resources/fraud-risk-tools---cso/fraud-risk-management-guide>



# Guía de Gestión de Riesgo de Fraude – COSO (2023)

## Summary of Fraud Risk Management Components and Principles

### Fraud Risk Governance

Fraud risk governance is an integral component of corporate governance and the internal control environment. Corporate governance addresses the manner in which the board of directors and management meet their respective obligations to achieve the organization's goals, including its fiduciary,

reporting, and legal responsibilities to stakeholders. The internal control environment creates the discipline that supports the assessment of risks to the achievement of the organization's goals.



**Principle 1** The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding management

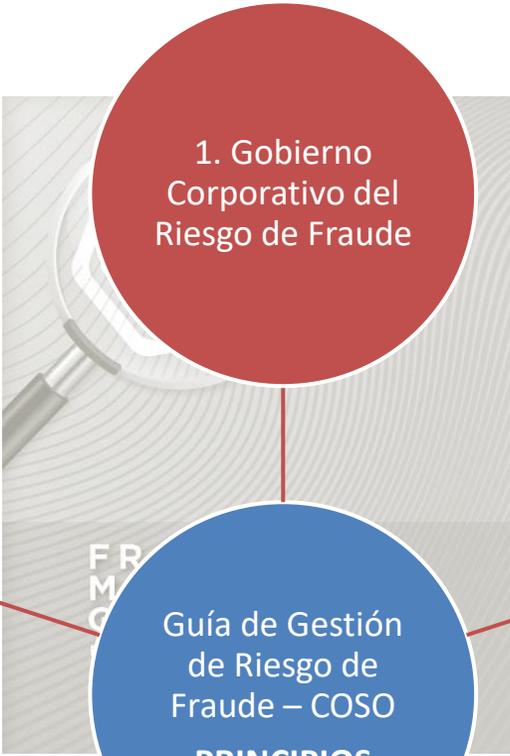
### Fraud Risk Assessments

A fraud risk assessment is a dynamic and iterative process for identifying and assessing fraud risks relevant to the organization. Fraud risk assessment addresses the risk of fraudulent financial reporting, fraudulent non-financial reporting, asset misappropriation, and corruption (including illegal acts and noncompliance with laws and regulations).

Organizations can tailor a fraud risk assessment to their individual needs. A fraud risk assessment is a process that is linked to COSO's



**Principle 2** The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.

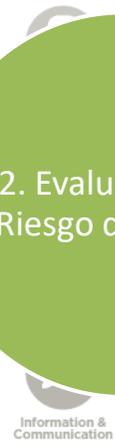


### Fraud Control Activity

A fraud control activity is an action established through policies and procedures that helps ensure that management's directives to mitigate fraud risks are carried out. A fraud control activity is a specific procedure or process intended either to prevent fraud from occurring or to detect fraud quickly in the event that it occurs.

Fraud control activities are generally classified as either preventive (designed to avoid a fraudulent event or transaction at the time of initial occurrence) or detective (designed to discover a fraudulent event or transaction

after the initial processing has occurred). The selection, development, implementation, and monitoring of fraud preventive and fraud detective control activities are crucial elements of managing fraud risk. Fraud control activities are documented with descriptions of the identified fraud risk and scheme, the fraud control activity that is designed to mitigate the fraud risk, and the identification of those responsible for the fraud control activity. Fraud control activities are integral to the ongoing fraud risk assessment component of internal control.



**Principle 3** The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.

Investigation against fraud allegations involving potential fraud and misconduct. An organization can improve its chances of loss recovery, while minimizing exposure to litigation and damage to reputation, by establishing and carefully preplanning investigation and corrective action processes.

The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

### Fraud Risk Management Monitoring Activities

The fifth fraud risk management principle relates to monitoring the overall Fraud Risk Management Program. Organizations use fraud risk management monitoring activities to ensure that each of the five principles of fraud risk management is present, designed, and that the organization is operating in a timely manner.

Organizations evaluate the effectiveness of each of the five principles of fraud risk management and communicate this information in a timely manner to parties responsible for fraud risk management, including senior management and the board of directors.

Similar to the COSO 2013 IC framework, organizations in a Fraud Risk Management Program that are built into the organization's business processes at varying levels provide timely information. In contrast, organizations conduct evaluations periodically that vary in frequency based on numerous factors, including the nature of the evaluations.

The organization selects, develops, and performs fraud control activities for each of the five principles of fraud risk management and communicates this information in a timely manner to parties responsible for fraud risk management, including senior management and the board of directors.

Fuente: <https://www.acfe.com/fraud-resources/fraud-risk-tools---cso/fraud-risk-management-guide>

## 2. Tecnología aplicada a la GRF



## 2. Tecnología aplicada a la GRF

---

- ▶ **La transformación digital y el desarrollo de las tecnologías disruptivas** están fortaleciendo muchos aspectos en las organizaciones (para realizar tareas mejor y más rápido), esto incluye los esfuerzos en la lucha contra el fraude.
- ▶ **La tecnología es una herramienta, y como tal puede ser utilizada para el bien o para el mal**, los deshonestos la está utilizando a su favor, es por ello que los honestos debemos considerar y optimizar el uso de la tecnología como una poderosa herramienta anti-fraude.

## 2. Tecnología aplicada a la GRF

**Hallazgos Clave**  
– Informe de evaluación comparativa  
de tecnología antifraude de 2024



Fuente:

<https://www.acfe.com/acfe-insights-blog/blog-detail?s=insights-from-2024-anti-fraud-technology-benchmarking-report>

## 2. Tecnología aplicada a la GRF

### Hallazgos clave



Nueve de cada 10 organizaciones (91%) utilizan **TÉCNICAS DE ANÁLISIS DE DATOS** como parte de sus programas antifraude.

91%

77%

Los **DATOS ESTRUCTURADOS INTERNOS** son la fuente de datos más común para el análisis, y el 77% de las organizaciones confían en este enfoque tradicional.



PURCHASING

41%

Las áreas de riesgo más comunes monitoreadas por el análisis de datos son **DESEMBOLSOS (44%)** y **COMPRAS (41%)**.



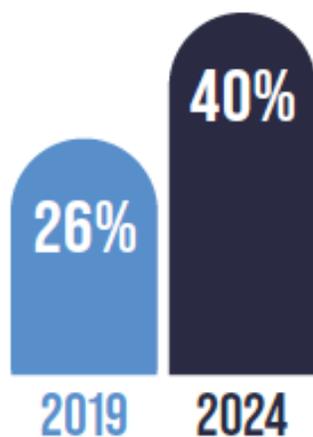
Fuente:  
<https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report>

## 2. Tecnología aplicada a la GRF

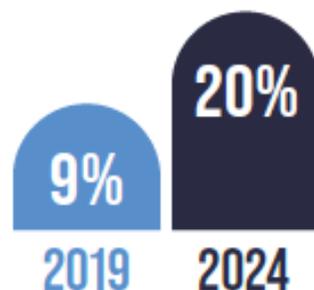
### Hallazgos clave

El uso tanto de la **BIOMÉTRICA** como de la **ROBÓTICA** en programas antifraude ha aumentado constantemente en los últimos años.

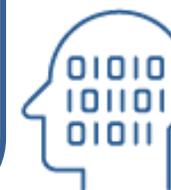
#### BIOMETRICS



#### ROBOTICS



Dos de cada cinco **organizaciones (40%)** utilizan actualmente la **BIOMÉTRICA FÍSICA** como parte de su programa antifraude, y otro **17% espera adoptar esta tecnología** en los próximos dos años.



40%

17%



Fuente:  
<https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report>

## 2. Tecnología aplicada a la GRF

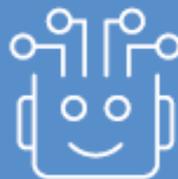
### Hallazgos clave

#### THE USE OF ARTIFICIAL INTELLIGENCE (AI) and MACHINE LEARNING

in anti-fraud programs is expected to nearly

# TRIPLE

over the next two years.



Se espera que **EL USO DE INTELIGENCIA ARTIFICIAL (IA) y APRENDIZAJE AUTOMÁTICO** en programas antifraude sea casi el **TRIPLE** en los próximos dos años.

# 83%

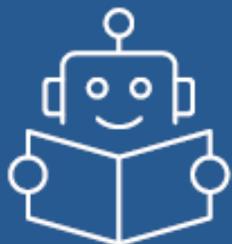
El **83%** de las organizaciones espera implementar **IA GENERATIVA** como parte de sus programas antifraude durante los próximos dos años.



Fuente:  
<https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report>

## 2. Tecnología aplicada a la GRF

### Hallazgos clave



**MORE THAN 50%  
OF ANTI-FRAUD PROGRAMS**

currently use or expect to adopt computer vision analysis, robotics, and behavioral biometrics at some point in the future.

**MÁS DEL 50% DE LOS PROGRAMAS ANTIFRAUDE** utilizan actualmente o esperan adoptar **análisis de visión por computadora, robótica y biometría del comportamiento** en algún momento en el futuro.

“La **visión por computadora** es un campo de la inteligencia artificial (IA) que utiliza el aprendizaje automático y las redes neuronales para enseñar a las computadoras y sistemas a obtener información significativa de imágenes digitales, videos y otras entradas visuales, y a hacer recomendaciones o tomar medidas cuando detectan defectos o problemas.”

<https://www.ibm.com/topics/computer-vision>

“La **biometría del comportamiento** mide y distingue de forma única patrones en el comportamiento de los usuarios de dispositivos. La biometría del comportamiento son hábitos y tendencias que los humanos desarrollan con el tiempo, dadas sus interacciones con diferentes dispositivos.”

<https://risk.lexisnexis.com/global/en/insights-resources/article/what-is-behavioral-biometrics#:~:text=Definition%3A%20Behavioral%20biometrics%20measures%20and,their%20interactions%20with%20different%20devices.>

“La **automatización robótica de procesos (Robotic Process Automation o RPA)** está transformando la manera de operar de las compañías. Los robots de software de RPA se comunican con los sistemas y las aplicaciones para agilizar procesos y reducir la carga de trabajo que recae sobre los humanos.”

[https://www.iberdrola.com/innovacion/rpa-que-es#:~:text=La%20automatizaci%C3%B3n%20rob%C3%B3tica%20de%20procesos%20\(Robotic%20Process%20Automation%20o%20RPA,que%20recae%20sobre%20los%20humanos.](https://www.iberdrola.com/innovacion/rpa-que-es#:~:text=La%20automatizaci%C3%B3n%20rob%C3%B3tica%20de%20procesos%20(Robotic%20Process%20Automation%20o%20RPA,que%20recae%20sobre%20los%20humanos.)



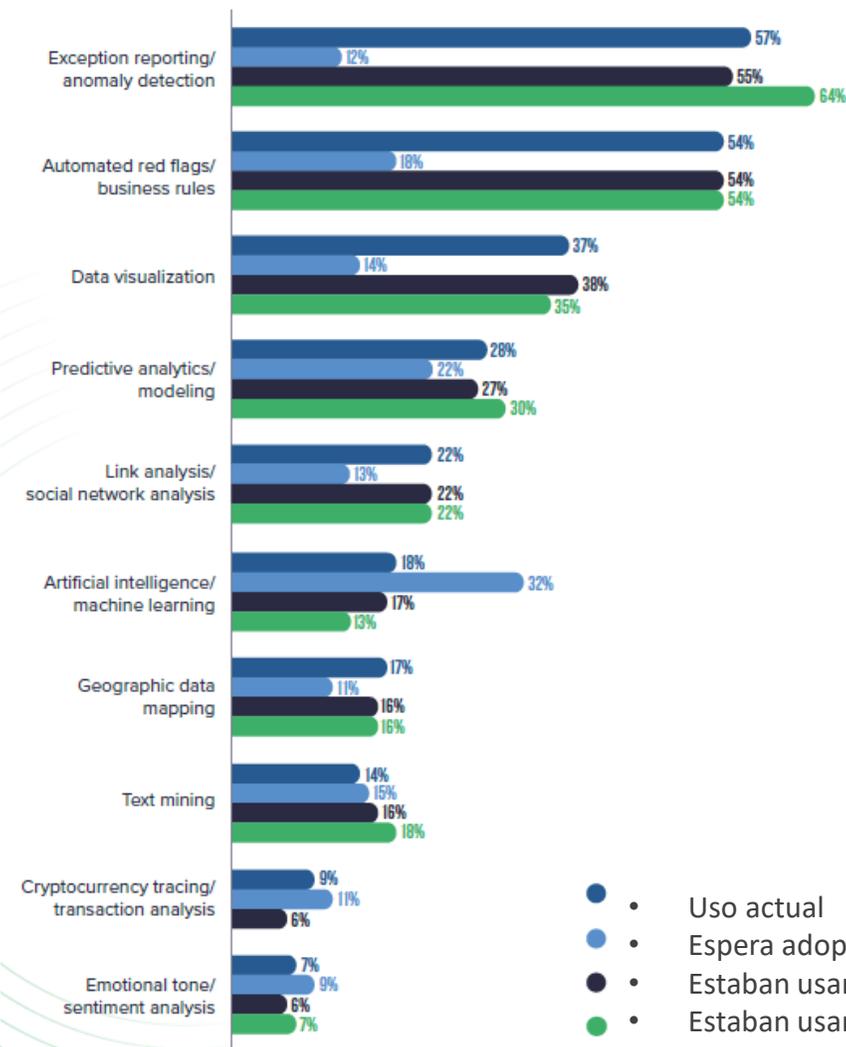
Fuente:  
<https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report>

## 2. Tecnología aplicada a la GRF

FIG. 1

¿Qué técnicas de análisis de datos utilizan las organizaciones para luchar contra el fraude?

- Informes de excepción/Detección de anomalías
- Banderas rojas automatizadas/reglas del negocio
- Visualización de datos
- Análisis predictivo/modelado
- Análisis de enlaces/análisis de redes sociales
- Inteligencia artificial/aprendizaje automático
- Mapeo de datos geográficos
- Minería de textos
- Seguimiento de criptomonedas/análisis de transacciones
- Tono emocional/análisis de sentimientos



- Uso actual
- Espera adoptar en los próximos 1 o 2 años
- Estaban usando en 2022
- Estaban usando en 2019



Fuente:  
<https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report>

Junio – 2025

## 2. Tecnología aplicada a la GRF

FIG. 2

¿Cuáles son los programas más utilizados para cada técnica analítica?



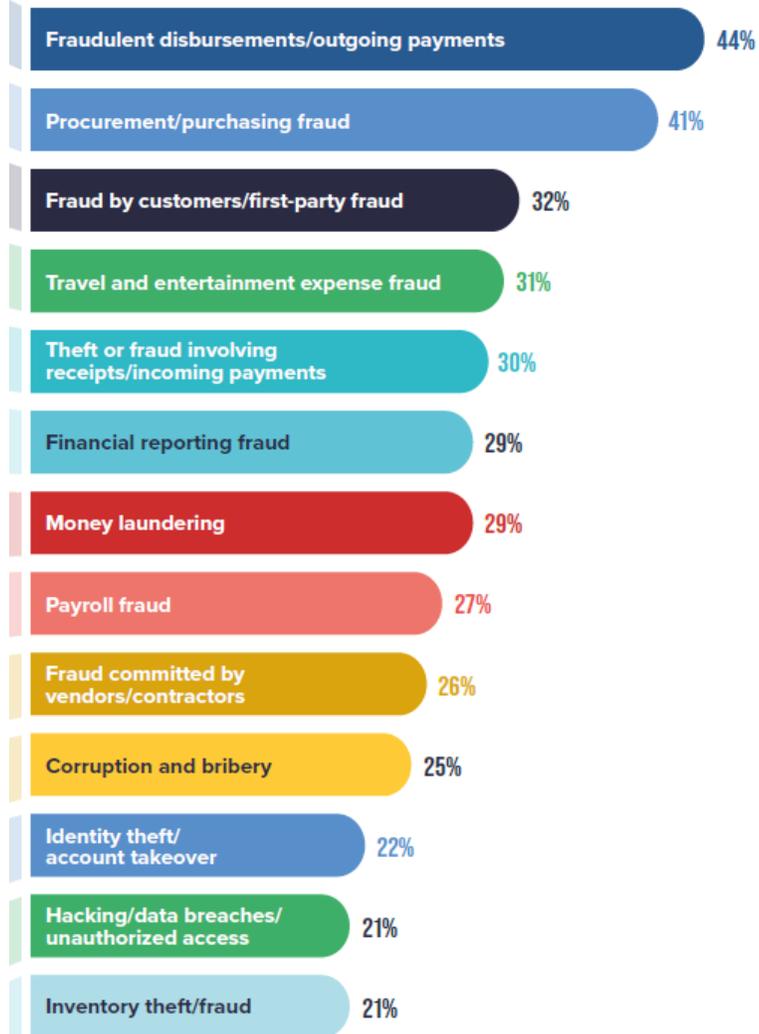
Fuente:  
<https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report>

## 2. Tecnología aplicada a la GRF

FIG. 3

¿En qué áreas de riesgo las organizaciones utilizan el análisis de datos para monitorear el fraude?

- Desembolsos/pagos efectuados fraudulentos
- Fraude en adquisiciones/compras
- Fraude por parte de clientes/fraude propio
- Fraude en gastos de viajes y entretenimiento
- Robo o fraude que involucre recibos/pagos entrantes
- Fraude de informes financieros
- Lavado de dinero
- Fraude de nómina
- Fraude cometido por proveedores/contratistas
- Corrupción y soborno
- El robo de identidad/apropiación de cuenta
- Hacking/violaciones de datos/ Acceso no autorizado
- Robo/fraude de inventario



Fuente:  
<https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report>

## 2. Tecnología aplicada a la GRF

---

### e-Discovery

#### Copilot

- ▶ *e-Discovery (o descubrimiento electrónico) es el proceso mediante el cual se identifica, recopila, analiza y presenta información almacenada electrónicamente (ESI) con fines legales, como litigios, investigaciones internas o auditorías regulatorias.*
- ▶ **¿Qué tipo de información se incluye?**
  - ▶ - Correos electrónicos y archivos adjuntos
  - ▶ - Documentos digitales (PDF, Word, Excel, etc.)
  - ▶ - Mensajes en redes sociales
  - ▶ - Registros de llamadas, mensajes de texto
  - ▶ - Archivos multimedia (audio, video, imágenes)
  - ▶ - Datos de aplicaciones empresariales y bases de datos
- ▶ **¿Para qué se utiliza?**
  - ▶ *El e-Discovery es fundamental en procesos judiciales y regulatorios, ya que permite a las partes involucradas acceder a evidencia digital relevante. También se usa en investigaciones internas para detectar fraudes, filtraciones de información o incumplimientos normativos.*



## 2. Tecnología aplicada a la GRF

FIG. 8

¿Las organizaciones utilizan software forense digital/e-discovery?

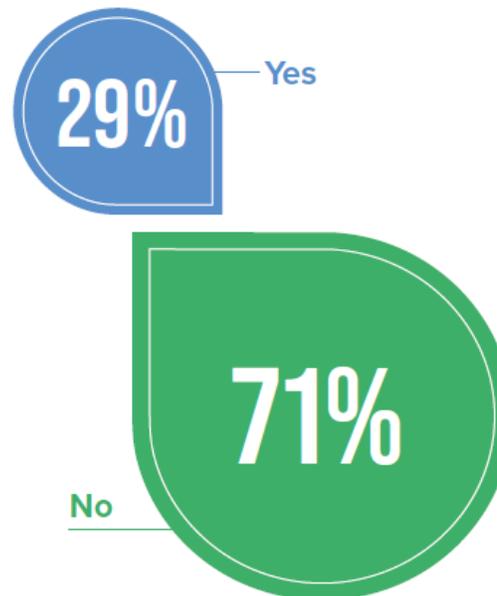


FIG. 9

¿Cuáles son los programas de software de descubrimiento electrónico/forense digital más comunes?



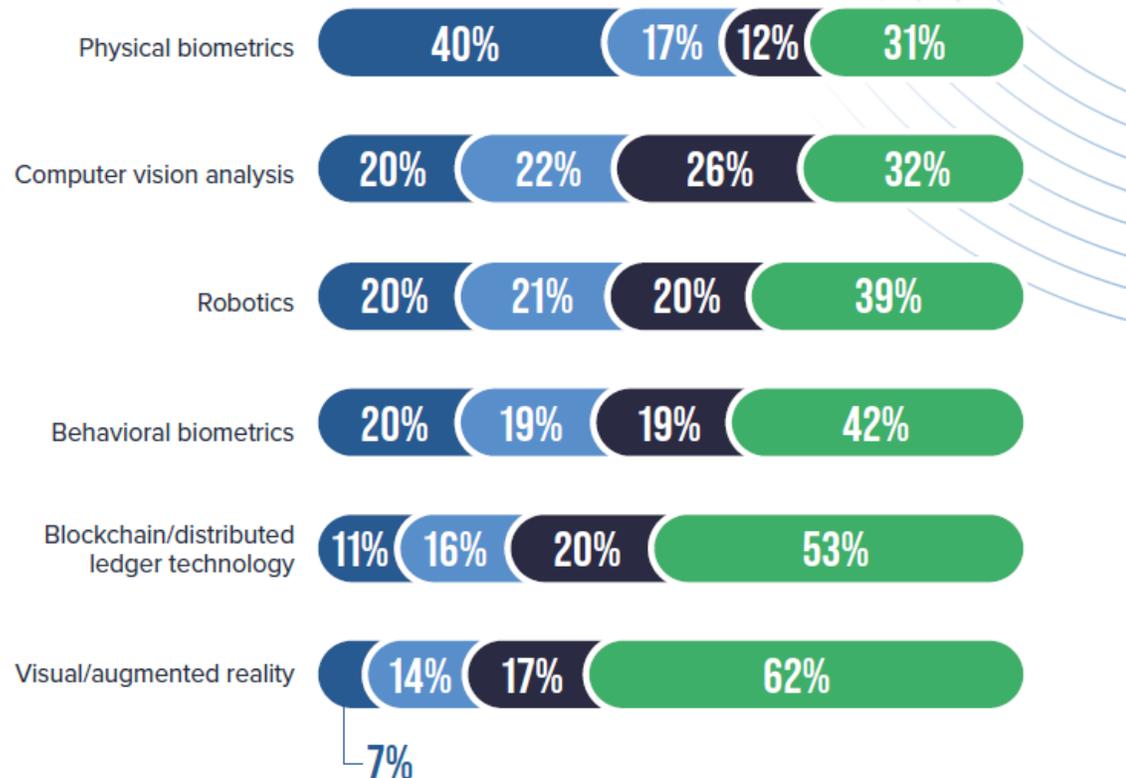
Fuente:  
<https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report>

## 2. Tecnología aplicada a la GRF

FIG. 12

¿Qué tecnologías emergentes están utilizando las organizaciones para luchar contra el fraude?

- Biometría física
- Análisis de visión por computadora
- Robótica
- Biometría del comportamiento
- Cadena de bloques/tecnología de contabilidad distribuida
- Realidad visual/aumentada



● Actualmente use   ● Do not currently use, but expect to deploy in the next 1–2 years  
 ● Do not currently use, but expect to deploy more than 2 years from now   ● Do not expect to use

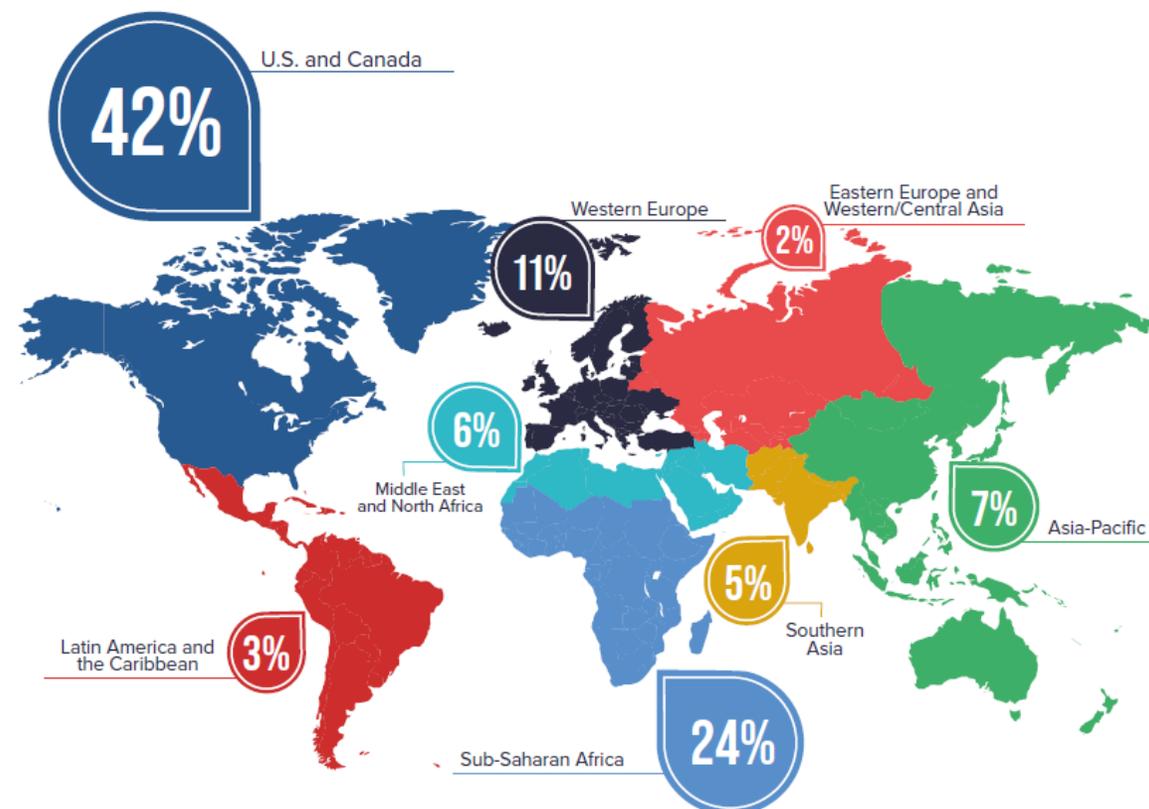


Fuente:  
<https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report>

## 2. Tecnología aplicada a la GRF

FIG. 20

Región de las organizaciones encuestadas



Fuente:  
<https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report>

**XIII**

Seminario Internacional  
de Auditoría Interna

## 3. Sistema de alertas para la detección de riesgos de fraude



## 2. Tecnología aplicada a la GRF

---

Sistema de alertas para la detección de riesgos de fraude – Análisis de Datos

## 3. Sistema de alertas para la detección de riesgos de fraude

---

### Sistema de alertas para la detección de riesgos de fraude

- ▶ Sistemas (herramientas, plataformas, tecnologías) de **análisis de datos** que permiten **identificar Indicadores Clave de Riesgo (KRI)**, para fines de **prevenir y detectar** situaciones irregulares (posibles casos de fraude).
  - ▶ Periódico
  - ▶ Continuo (en tiempo real)
- ▶ **KRI enfocados en**, transacciones, situaciones, comportamientos:
  - ▶ Extraños
  - ▶ Atípicos
  - ▶ Sospechosos

## 3. Sistema de alertas para la detección de riesgos de fraude

---

### Sistema de alertas para la detección de riesgos de fraude

#### ▶ Ejemplos de KRI

##### ▶ **Factura #1**

- ▶ **Precio unitario superior en X% comparado** con el precio unitario de la compra anterior y/o del promedio de las compras de los últimos X meses
- ▶ **Aumento del “sueldo base”** superior al X%
- ▶ **Fraccionamiento de compras**, sobre la base de compras a un mismo proveedor en un periodo de X días, que acumuladas sobrepasen un monto \$X
- ▶ **Ciente único**, sobre la base de que un proveedor emita tres facturas secuenciales

### 3. Sistema de alertas para la detección de riesgos de fraude

---

## Sistema de alertas para la detección de riesgos de fraude

- ▶ Determinación de KRI para ejecutar análisis de datos:
  - ▶ Objetivo del indicador
  - ▶ Fuentes de información (confiables, accesibles)
  - ▶ Afinar el indicador (para descartar lo más posible “falsos positivos”)
  - ▶ Determinar frecuencia de ejecución

### 3. Sistema de alertas para la detección de riesgos de fraude

#### Sistema de alertas para la detección de riesgos de fraude



# Sistema de alertas para la detección de riesgos de fraude – Herramientas

### 3. Sistema de alertas para la detección de riesgos de fraude



Controles  
de proceso

- ▶ **Programas de auditoría continua**
  - ▶ Datos/transacciones: inusuales, atípicos, extraños
  - ▶ Tecnología de la información & tecnología de la operación
  - ▶ Enfoque
    - ▶ Indicadores clave de riesgo KRI
    - ▶ Efectividad del control KPI
  - ▶ Ejemplo de KRIs: factura 1, fraccionamiento de compras, cambios en archivos maestros, cotejar archivos maestros, incremento inusual de precio unitario, incremento inusual de sueldo base

## 3. Sistema de alertas para la detección de riesgos de fraude



Controles  
de proceso

- ▶ **Análisis avanzado de datos**
  - ▶ Comportamientos
  - ▶ Tendencias
  - ▶ Relaciones
  - ▶ Transacciones sospechosas
  - ▶ Cruces de bases de datos

### 3. Sistema de alertas para la detección de riesgos de fraude



Controles  
de proceso

- ▶ Sistemas de **compliance** para debidas diligencias
  - ▶ Clientes
  - ▶ Proveedores
  - ▶ Empleados
- ▶ Sistemas de análisis y monitoreo (periódico / continuo) **compliance** (empleados versus proveedores)
  - ▶ Conflicto de intereses
  - ▶ Vinculaciones PEP
- ▶ Sistemas de gestión de **riesgos de terceros**

### 3. Sistema de alertas para la detección de riesgos de fraude



Controles  
de proceso

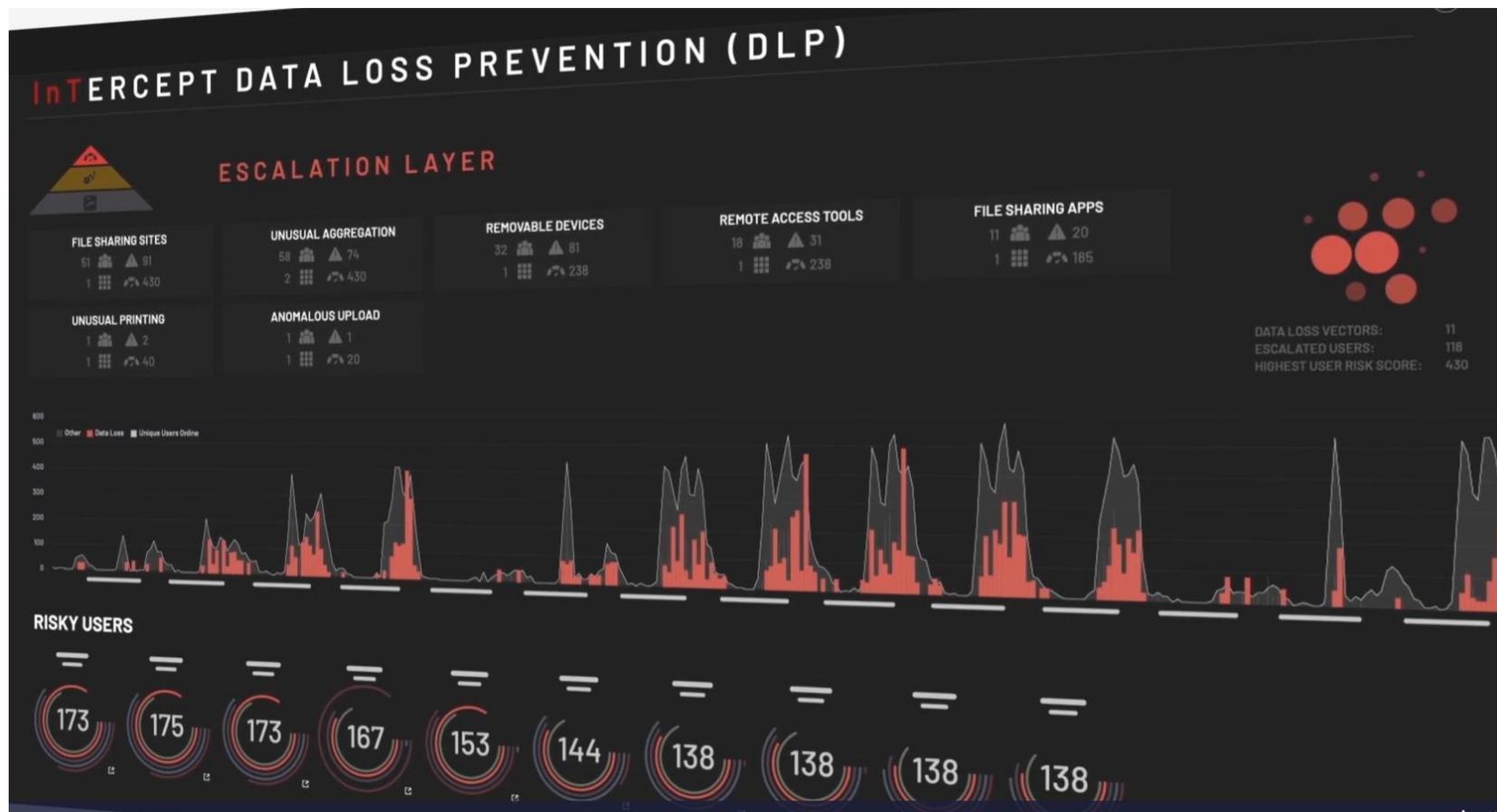
- ▶ **Sistemas de rendición de gastos**
  - ▶ Gastos de viaje
  - ▶ Tarjetas de crédito
  - ▶ Cajas chicas
  - ▶ Fondos reembolsables
- ▶ **Sistemas de declaraciones**
  - ▶ Conflictos de interés
  - ▶ Regalos y entretenimiento
- ▶ **Sistemas de registros / bitácoras**
  - ▶ Reuniones con funcionarios públicos

### 3. Sistema de alertas para la detección de riesgos de fraude

- ▶ Sistemas avanzados de análisis de comportamientos biométrico sospechoso



Procedimientos  
proactivos



Ejemplo ilustrativo

<https://www.dtexsystems.com/solutions/behavioral-dlp/>

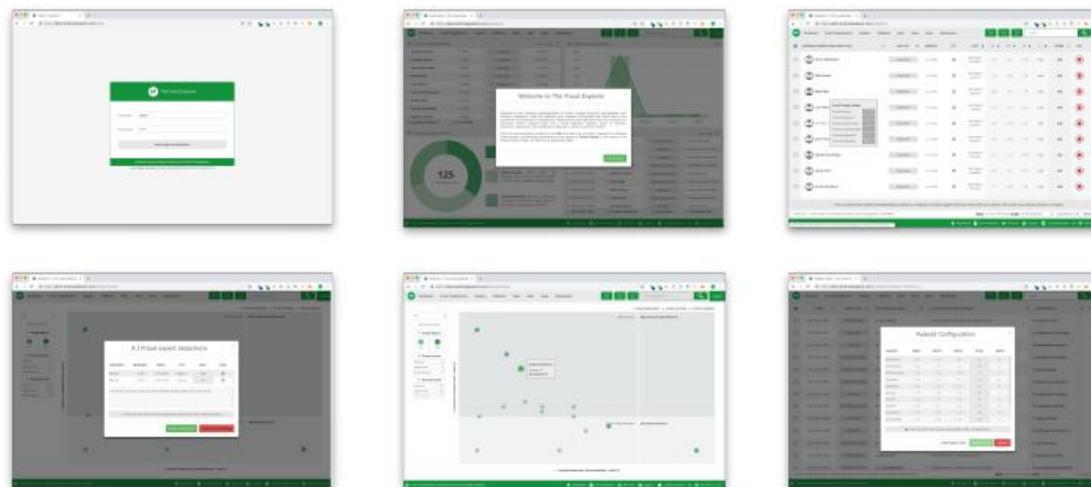
### 3. Sistema de alertas para la detección de riesgos de fraude

- ▶ **Análisis de comunicaciones sospechosas (en base al triángulo del fraude)**



Procedimientos  
proactivos

#### PANTALLAZOS APARIENCIA FRONTEND



The Fraud Explorer © Opensource Fraud Triangle Analytics

Ejemplo ilustrativo

[https://www.thefraudexplorer.com/files/The\\_Fraud\\_Explorer\\_Datasheet.pdf](https://www.thefraudexplorer.com/files/The_Fraud_Explorer_Datasheet.pdf)

### 3. Sistema de alertas para la detección de riesgos de fraude



Procedimientos  
proactivos

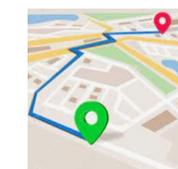
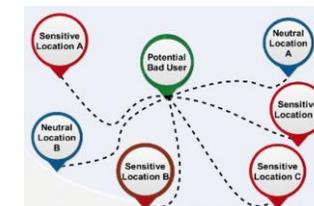
- ▶ Sistemas de gestión de riesgos, aplicados a gestión de riesgos de fraude
- ▶ Auditorías sorpresa
- ▶ Revisiones proactivas de fraude (auditorías de fraude) 
- ▶ Sistemas de gestión de riesgos, aplicados a gestión de riesgos de fraude

### 3. Sistema de alertas para la detección de riesgos de fraude



Otros usos de  
 innovación y  
 tecnología

- ▶ Uso de **inteligencia artificial** para validar información en tiempo real (por ejemplo firmas de cheques)
- ▶ **Análisis de comportamientos y tendencias** para validaciones en tiempo real (por ejemplo hábitos de compra en tarjetas de crédito)
- ▶ **Tableros de control (dashboard)** y centros de inteligencia (control rooms) con alertas en tiempo real
- ▶ Análisis de **reconocimiento facial** como señal de alerta (pilotos en retail)
- ▶ Análisis de **comportamiento de flotas** en base a GPSs con alertas en tiempo real (minería)



### 3. Sistema de alertas para la detección de riesgos de fraude



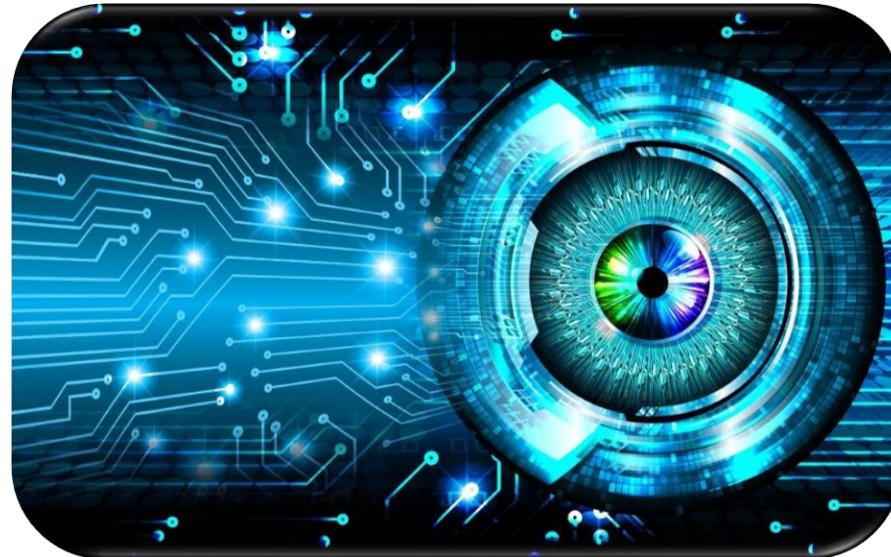
Otros usos de  
innovación y  
tecnología

- ▶ **Lentes inteligentes** para visitas presenciales o en remoto
- ▶ Vigilancia con **drones** industriales (instalaciones, inventarios)
- ▶ Sistemas de **control de consumo de combustible** (anillos, configuraciones, restricciones, alertas, reportes)
- ▶ **Cámaras** de vigilancia, con visión artificial
- ▶ Tecnología aplicada a la **seguridad industrial**



### 3. Sistema de alertas para la detección de riesgos de fraude

Visión artificial – Antifraude



## 3. Sistema de alertas para la detección de riesgos de fraude

### Visión artificial

- ▶ **Computer Vision (visión artificial)** es una disciplina de la inteligencia artificial que se enfoca en permitir que las computadoras "vean" e interpreten imágenes y vídeos.
- ▶ En esencia, busca que las **máquinas puedan percibir, analizar y comprender el mundo visual** de la misma manera que los humanos. Esto implica desarrollar algoritmos que puedan identificar objetos, rostros, escenas, y otros elementos visuales en imágenes y vídeos, permitiendo a las computadoras tomar decisiones y realizar acciones basadas en esa información.



## 3. Sistema de alertas para la detección de riesgos de fraude

### Visión artificial



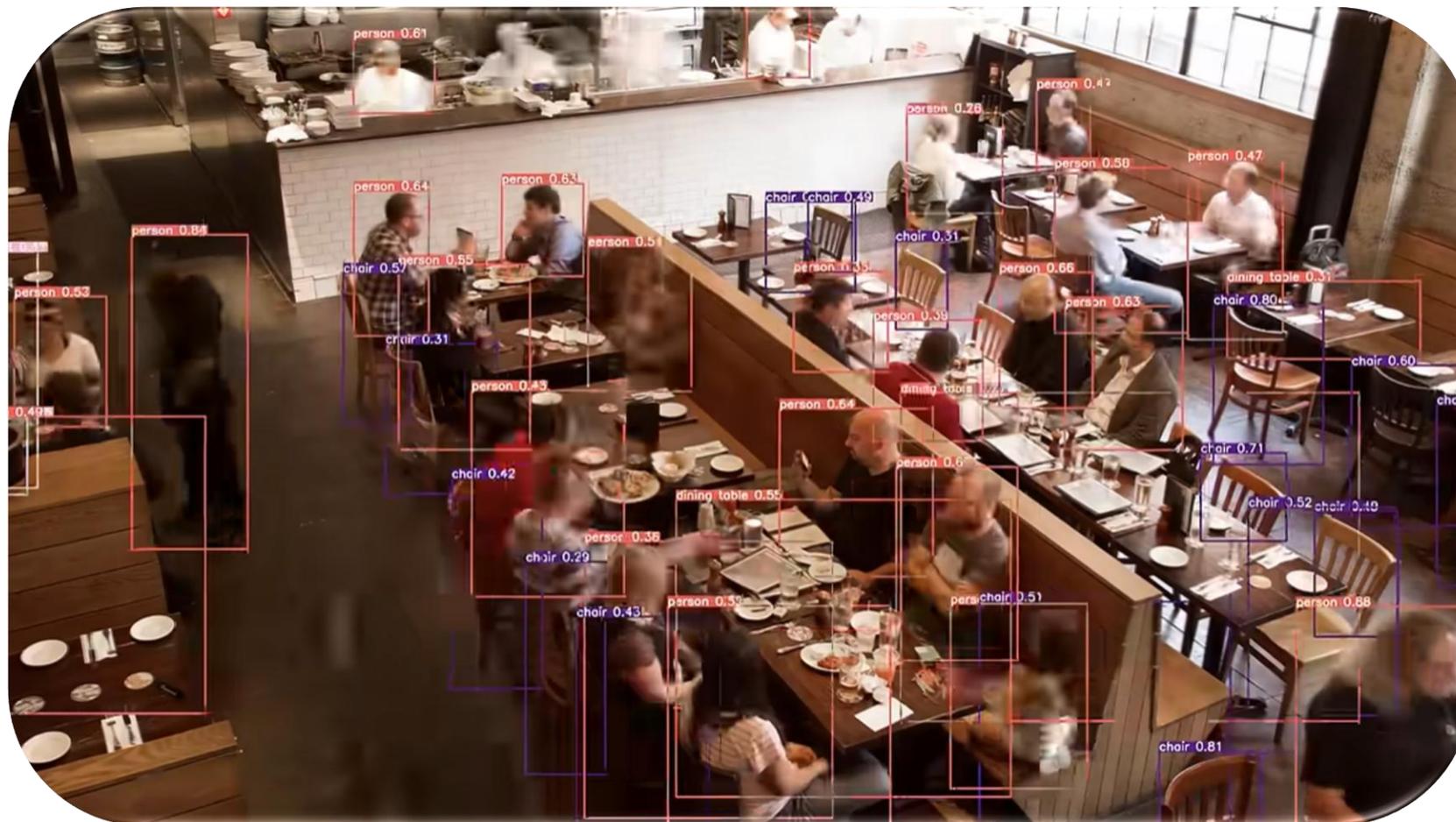
Video 1

Fuente:

[https://www.youtube.com/watch?v=y\\_psKxkY9A8](https://www.youtube.com/watch?v=y_psKxkY9A8)

# 3. Sistema de alertas para la detección de riesgos de fraude

## Visión artificial



**Video 2**

Fuente:  
[https://www.youtube.com/watch?v=i\\_mL3LT0IDg](https://www.youtube.com/watch?v=i_mL3LT0IDg)

## 3. Sistema de alertas para la detección de riesgos de fraude

---

### VISIÓN ARTIFICIAL

**Prompt:** “Cómo utilizar visión artificial como una herramienta antifraude en una organización”

#### Copilot

- ▶ *La **visión por computadora** se ha convertido en una poderosa aliada en la lucha contra el fraude, especialmente en sectores como banca, seguros, retail y logística.*
- ▶ *Esta tecnología permite analizar imágenes y videos en tiempo real para detectar comportamientos sospechosos, falsificaciones o accesos no autorizados.*



## 3. Sistema de alertas para la detección de riesgos de fraude

---

### VISIÓN ARTIFICIAL

#### Copilot

##### ▶ *Aplicaciones antifraude con visión artificial*

###### ▶ *Reconocimiento facial para control de identidad*

*Se utiliza en cajeros automáticos, accesos físicos o plataformas digitales para verificar que el usuario sea quien dice ser. Esto previene suplantaciones de identidad o accesos indebidos.*

###### ▶ *Detección de documentos falsificados*

*Algoritmos entrenados pueden identificar alteraciones en cédulas, pasaportes, licencias o facturas escaneadas, comparando patrones visuales con bases de datos oficiales.*

###### ▶ *(...)*



## 3. Sistema de alertas para la detección de riesgos de fraude

---

### VISIÓN ARTIFICIAL

#### Copilot

- ▶ **Aplicaciones antifraude con visión artificial**

- ▶ (...)

- ▶ **Análisis de comportamiento en video vigilancia**

- En tiendas o bancos, la visión por computadora puede detectar movimientos inusuales como manipulación de cámaras, accesos fuera de horario o patrones de robo interno.*

- ▶ **Validación de firmas manuscritas**

- Se puede analizar la presión, trazo y velocidad de una firma para verificar su autenticidad, útil en contratos o autorizaciones físicas.*

- ▶ **Prevención de fraude en seguros**

- Por ejemplo, al analizar imágenes de accidentes automovilísticos para detectar inconsistencias entre el daño reportado y el daño real del vehículo.*



## 3. Sistema de alertas para la detección de riesgos de fraude

---

### VISIÓN ARTIFICIAL

#### Copilot

- ▶ *Ejemplo real*
- ▶ *Una aseguradora implementó visión por computadora para analizar fotos de siniestros. El sistema detectó que **varios clientes enviaban imágenes de daños idénticos en diferentes reclamos**. Gracias a esto, se evitó el pago de indemnizaciones fraudulentas y se fortaleció el proceso de validación.*



### 3. Sistema de alertas para la detección de riesgos de fraude

## Biometría conductual - - Antifraude



### 3. Sistema de alertas para la detección de riesgos de fraude

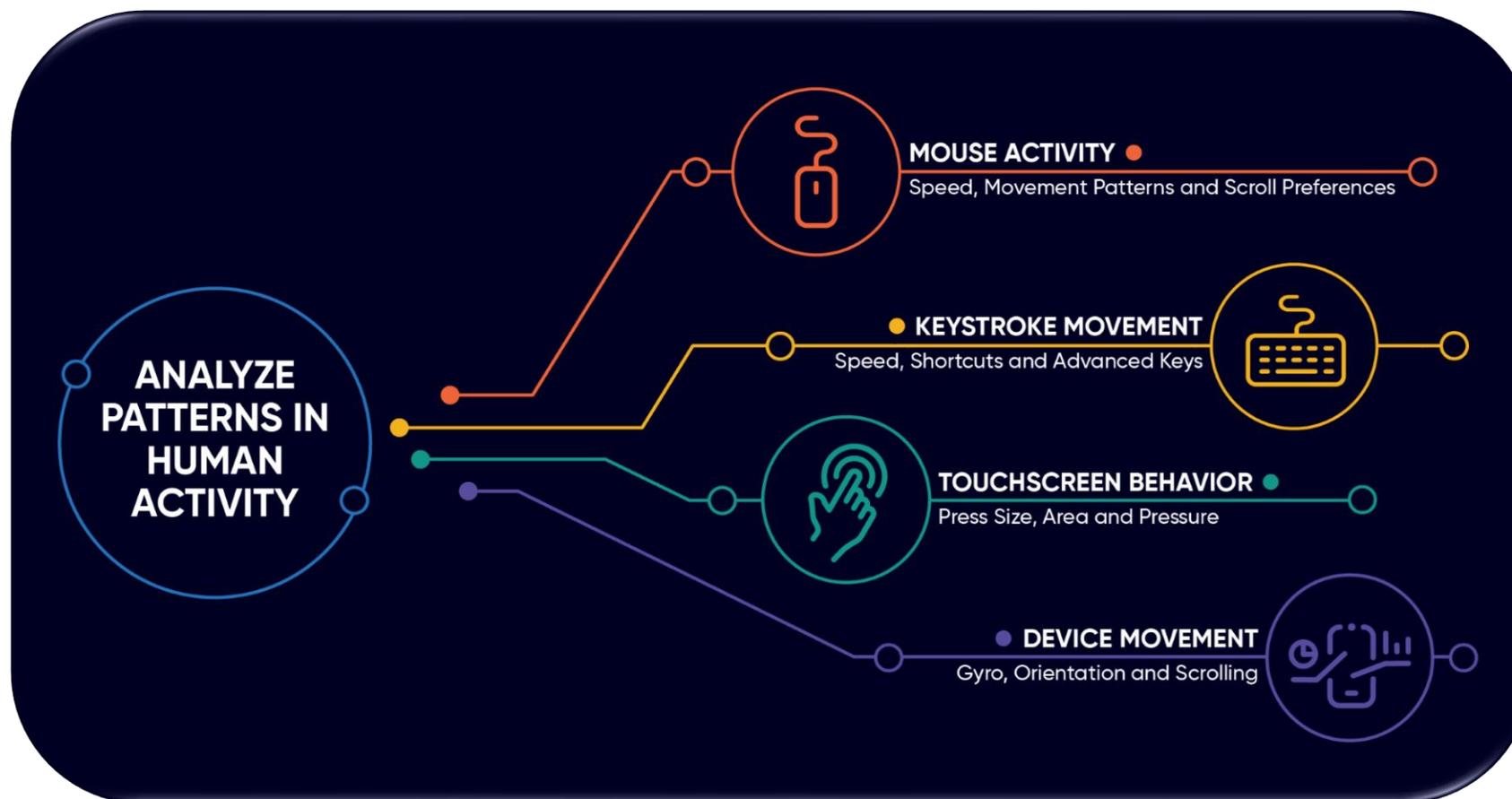
#### Biometría conductual

- ▶ La biometría conductual (behavioral biometrics) es un tipo de identificación que analiza los patrones de comportamiento de una persona para confirmar su identidad.
- ▶ En lugar de usar datos físicos como huellas dactilares, esta técnica evalúa cómo interactúa una persona con un dispositivo o sistema, como el teclado o el movimiento del mouse.



## 3. Sistema de alertas para la detección de riesgos de fraude

### Biometría conductual



Fuente:  
<https://www.biocatch.com/blog/what-is-behavioral-biometrics>

# 3. Sistema de alertas para la detección de riesgos de fraude

## Biometría conductual



Video 3

Fuente:  
<https://www.dtexsystems.com/capabilities/behavioral-dlp/>

## 3. Sistema de alertas para la detección de riesgos de fraude

### Monitoreo de Comportamiento biométrico



## Video 4

Fuente:

<https://risk.lexisnexis.com/global/en/products/behaviosec>

## 3. Sistema de alertas para la detección de riesgos de fraude

---

### VISIÓN ARTIFICIAL

**Prompt:** “Cómo utilizar biometría del comportamiento como una herramienta antifraude en una organización”

#### Copilot

- ▶ *La biometría del comportamiento (behavioral biometrics) es una tecnología antifraude emergente que **analiza cómo interactúan los usuarios con dispositivos y plataformas digitales**, en lugar de qué datos ingresan.*
- ▶ *Es invisible para el usuario, difícil de falsificar y altamente efectiva para detectar accesos no autorizados o suplantaciones de identidad.*



# 3. Sistema de alertas para la detección de riesgos de fraude

## VISIÓN ARTIFICIAL

### Copilot

#### ▶ *¿Cómo funciona?*

- ▶ *Se basa en **patrones únicos de comportamiento** como:*
  - ▶ *- Dinámica de escritura: velocidad, ritmo y presión al teclear.*
  - ▶ *- Uso del ratón o pantalla táctil: trayectorias, clics, presión y velocidad.*
  - ▶ *- Forma de sostener el dispositivo móvil: inclinación, orientación, aceleración.*
  - ▶ *- Interacción con la interfaz: secuencia de navegación, tiempo en cada pantalla, gestos.*
- ▶ *Estos datos se procesan mediante inteligencia artificial para **crear un perfil conductual único por usuario**. Si en una sesión futura el comportamiento no coincide con el perfil, se genera una alerta o se bloquea la acción sospechosa.*



## 3. Sistema de alertas para la detección de riesgos de fraude

---

### VISIÓN ARTIFICIAL

#### Copilot

##### ▶ *Aplicaciones antifraude*

- ▶ *- **Prevención de apropiación de cuentas:** Detecta si alguien accede a una cuenta con credenciales robadas pero con un comportamiento diferente al del titular legítimo.*
- ▶ *- **Protección contra bots y scripts automatizados:** Identifica patrones no humanos en la interacción.*
- ▶ *- **Detección de fraude en apertura de cuentas:** Evalúa si el comportamiento durante el registro es típico de un usuario genuino o de un estafador.*
- ▶ *- **Mitigación de fraudes por ingeniería social:** Si un usuario legítimo está siendo manipulado, su comportamiento puede cambiar y ser detectado.*



## 3. Sistema de alertas para la detección de riesgos de fraude

---

### VISIÓN ARTIFICIAL

#### Copilot

- ▶ *Ejemplo real*
- ▶ *Dos bancos europeos de primer nivel implementaron biometría conductual en sus procesos de apertura de cuentas. Lograron **reducir significativamente los fraudes por suplantación**, al identificar desviaciones en el comportamiento esperado durante el registro.*



# Conclusión



## Conclusiones

---

- ▶ Considerar que la **tecnología es una “herramienta”**, que puede ser utilizada para el bien o para el mal
- ▶ **Aprovechar la tecnología ya existente** en la organización (gestión y control)
- ▶ **Considerar nuevas tecnologías** en cuanto a combatir el fraude (más allá de lo tradicional)

# Conclusiones

---

- ▶ Estamos en un mundo en constante cambio, un **cambio que, a diferencia de tiempos pasados, es más profundo y más rápido.**
- ▶ En ese contexto, las sociedades, las organizaciones, las profesiones, los marcos metodológicos, **todo en general está evolucionando, para atender nuevas y desafiantes realidades.**
- ▶ Dichos cambios también se están dando, se deben dar, **en el ámbito del “Control Interno” implementado en las organizaciones**, para lograr una adecuada cobertura frente a los riesgos existentes y riesgos emergentes, más relevantes, por su potencial impacto y probabilidad.
- ▶ En ese sentido, **la innovación y la tecnología son los principales IMPULSORES para mejorar y fortalecer el Control Interno en las organizaciones**, en esta nueva era, la era de la transformación digital.

---

# ¡Gracias por su atención!

## Preguntas



*“Hay tres grupos de personas: los que hacen que las cosas sucedan, los que miran las cosas que suceden, y aquellos que se preguntan qué sucedió”*

Nicholas Murray Butler

¡Muchas gracias por su atención!



**Jorge Badillo Ayala**



@jbadillo1975



jgba1975@hotmail.com



Contacto LinkedIn

<https://cl.linkedin.com/in/jorge-badillo-92121234>

# XII

Seminario Internacional  
de Auditoría Interna

## MÁS ALLÁ DEL RIESGO ¡ESTRATEGIAS EN ACCIÓN!

**Jorge Badillo**



# ¡Gracias!



Alcaldía de Medellín  
Distrito de  
Ciencia, Tecnología e Innovación