

Abril 2022

Nuestro estudio Global Economic Crime and Fraud Survey 2022 proporciona información sobre la amenaza, el costo del fraude y lo que las empresas deben hacer para desarrollar respuestas proactivas más fuertes. De acuerdo con la encuesta, los ataques cibernéticos encabezan la lista de principales delitos económicos y amenazas de fraude que enfrentan la gran mayoría de empresas en la actualidad. Cerca de la mitad de empresas encuestadas reportan haber experimentado algún tipo de fraude en los últimos 2 años.

[Leer más](#)

Global Economic Crime and Fraud Survey 2022

46% de organizaciones informaron haber experimentado fraude o delitos económicos en los últimos 24 meses

40% de las organizaciones que ha experimentado fraude ha sido en plataformas digitales

Riesgos emergentes:
Fraude en la presentación de informes ESG y el fraude en la cadena de suministro

2/3 de empresas víctimas de algún tipo de fraude son de los sectores de tecnología, medios de comunicación y telecomunicaciones

Principales perpetradores de las experiencias de fraudes más serias o disruptivas

 Perpetrador externo	 Perpetrador interno	 Colusión entre actores internos y externos
43%	31%	26%
(41% en 2020)	(38% en 2020)	(21% en 2020)

Las empresas más grandes corren un mayor riesgo de fraude:

El **52%** de las empresas encuestadas con ingresos anuales globales superiores a US\$10,000 millones, experimentó fraude durante los últimos 24 meses. Dentro de ese grupo, casi una de cada cinco informó que su incidente más perturbador tuvo un impacto financiero de más de US\$50 millones.

En empresas con menos de US\$100 millones de ingresos; el **38%** experimentó fraude, de las cuales una de cada cuatro se enfrentó a un impacto total de más de US\$1 millón.

3 acciones para proteger tu perímetro:

- 1**

Comprender el ciclo de vida por completo:

Identificar dónde existen oportunidades para que un defraudador se aproveche de los productos de cara al cliente y cause daños financieros, legales o de reputación

2

Conseguir el equilibrio adecuado:

Una buena experiencia de usuario como un control eficaz del fraude son posibles gracias a la combinación adecuada de tecnología, estrategia y procesos contra el fraude

3

Ordenar los datos:

Consolidar los datos de sistemas dispares y desconectados en una plataforma centralizada que pueda hacer un seguimiento del ciclo de vida de los usuarios de principio a fin (defraudadores o no) y generar alertas significativas

La pandemia y el crecimiento continuo de las plataformas digitales ha generado un aumento en el número de casos de fraude a nivel global. Guillermo Zapata, gerente senior de GRC de PwC Perú, explica en esta entrevista cuáles son los sectores más afectados y qué estrategias deben seguir para protegerse de este tipo de riesgo.

[Leer más](#)



Entrevista PwC

Guillermo Zapata

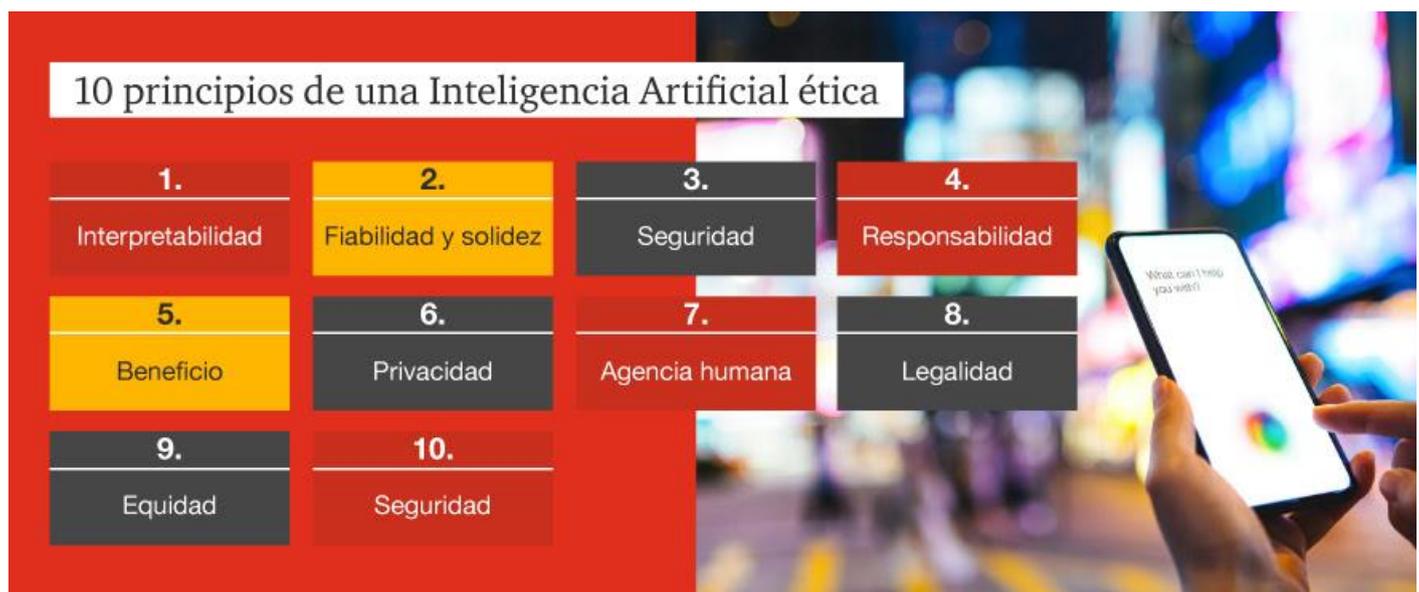
Gerente senior de GRC de PwC Perú

“El auge de las plataformas digitales abre la puerta a un mayor número de riesgos. Esto representa un cambio interesante, ya que el fraude se ha entendido tradicionalmente a través de una mirada financiera”.

Guillermo Zapata, a man in a blue suit with arms crossed, stands against a white background. To his right is a vertical yellow bar with a magnifying glass icon.

Crear Inteligencia Artificial ética reduce posibles riesgos para las empresas, pero no es una tarea fácil. La definición de IA ética difiere según a quién se pregunte y qué iniciativas se examinen. Identificamos diez principios básicos que cuentan con un amplio consenso a nivel mundial.

[Leer más](#)



10 principios de una Inteligencia Artificial ética

1. Interpretabilidad	2. Fiabilidad y solidez	3. Seguridad	4. Responsabilidad
5. Beneficio	6. Privacidad	7. Agencia humana	8. Legalidad
9. Equidad	10. Seguridad		

The infographic features a grid of 10 numbered principles on a red background. To the right, a hand holds a smartphone displaying a colorful chart against a blurred city night background.