CONSEJO CIUDADANO
PARA LA SEGURIDAD Y JUSTICIA
DE LA CIUDAD DE MÉXICO

# Riesgos y prevención ante la Inteligencia Artificial

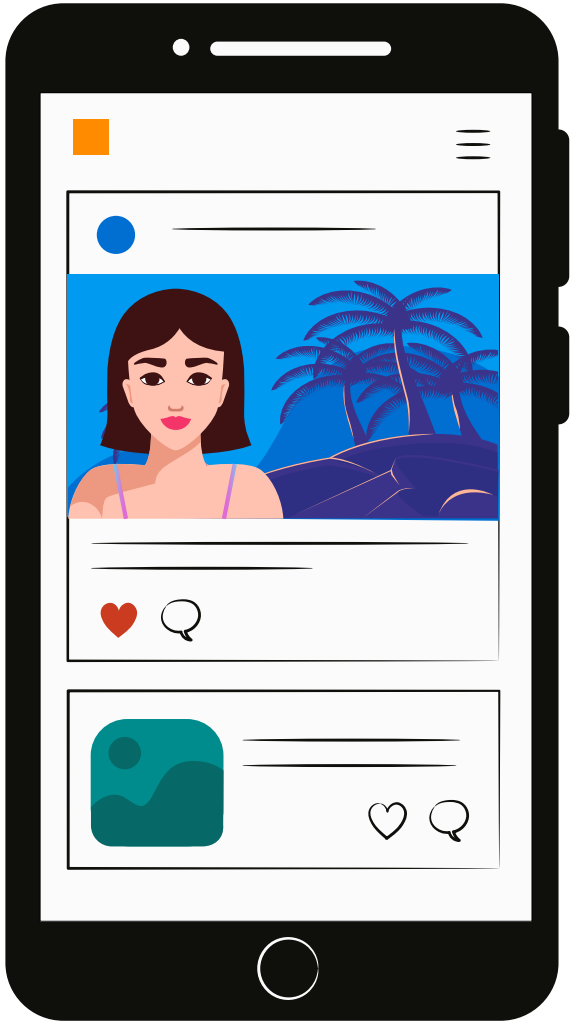
# El contexto de la IA

- La Inteligencia Artificial posibilita el acceso a temas y conexiones relevantes, así como representa **un riesgo de ser víctima** de desinformación, manipulación o delitos patrimoniales.

- Los delincuentes, a través del deepfake, **modifican videos, imágenes y audios** con la intención de robar identidad, defraudar o extorsionar.

# El contexto de la IA

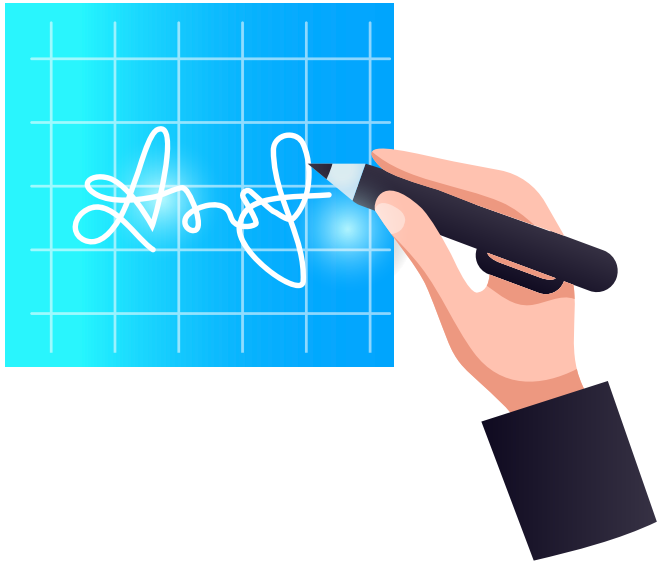
- Son herramientas de **fácil acceso y bajo costo.**
- Un extorsionador puede **enviar videos o audios manipulados** donde pareciera que una persona querida está en peligro inminente.
- Fotos, videos o audios pueden ser alterados para **crear circunstancias que afecten el patrimonio o reputación** de las personas.



# IA y robo de identidad

Los delincuentes acuden al **robo de identidad** para:

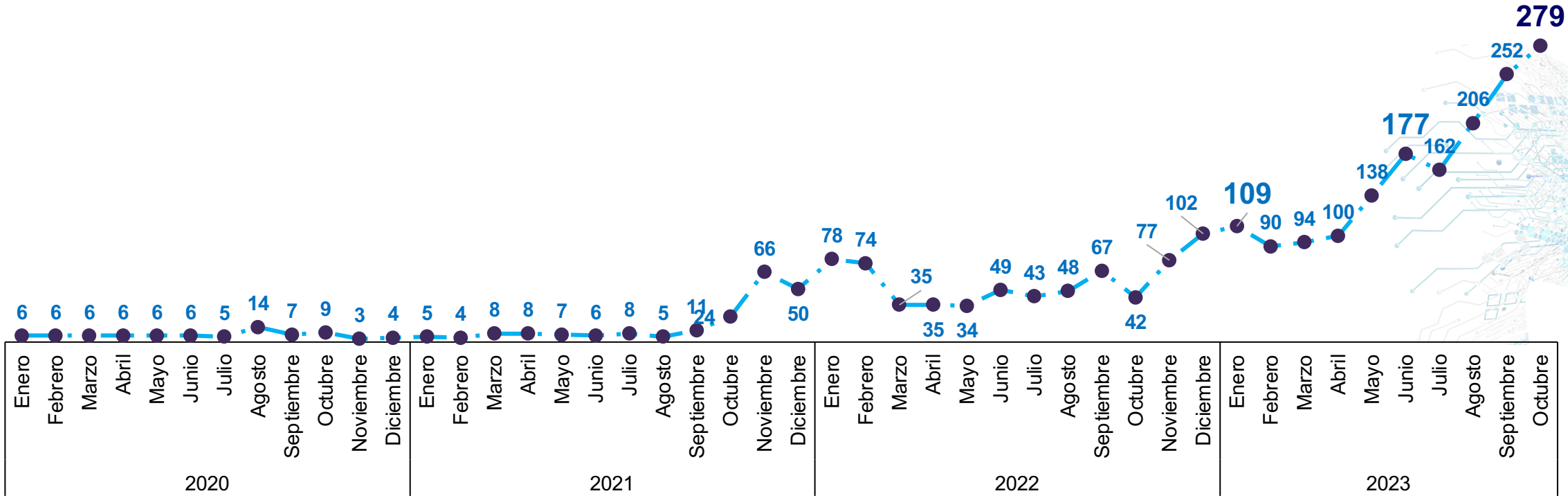
- **Tramitar tarjetas o cuentas bancarias** para pagar compras no realizadas por el dueño de la cuenta.
- **Acosar, abusar** laboral, profesional o sexualmente de una persona.
- Obtener más información de esa persona para vulnerarla aún más.
- En contextos de campañas políticas se contratan con agencias de comunicación para **falsificar la identidad de aquellos a quienes se quiere perjudicar**.



# Robo de Identidad

Los datos del Consejo Ciudadano revelan un **aumento en los reportes** por robo de identidad, que podría crecer ante el empleo del deepfake.

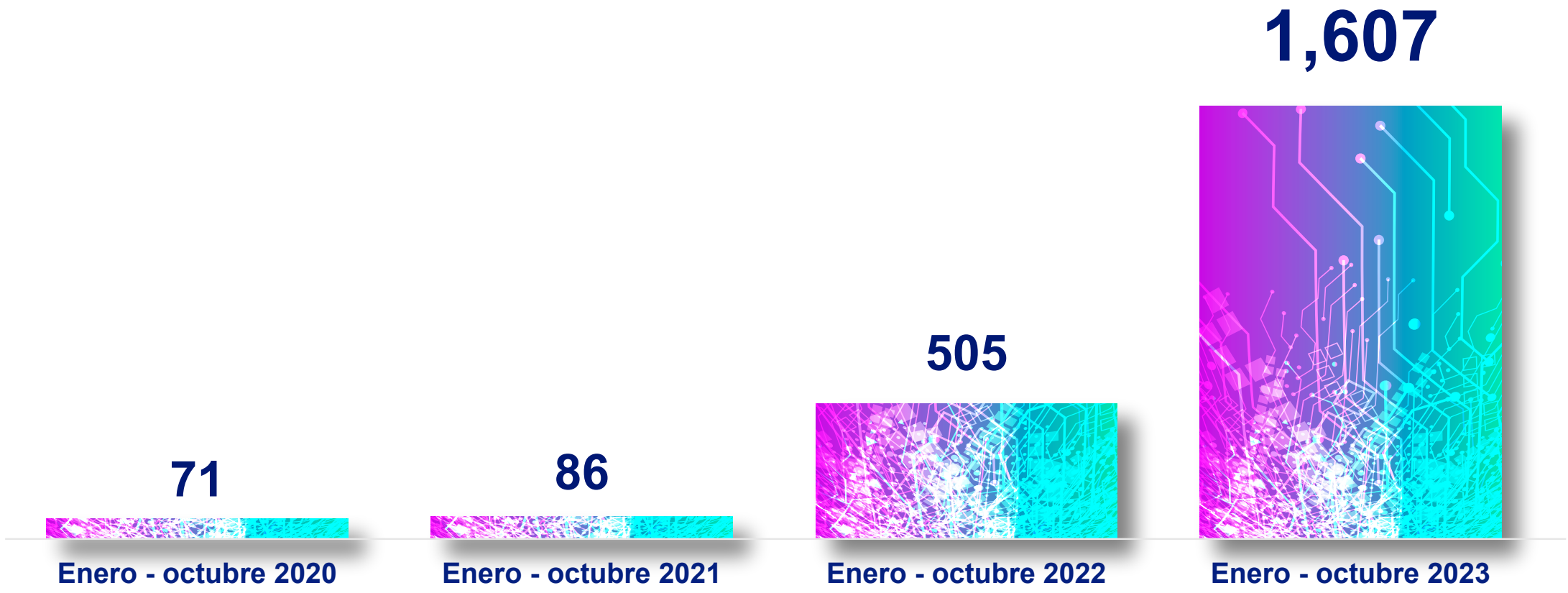
**2020: 78** | **2021: 202** | **2022: 684** | **2023: 1,607**




Fuente: Consejo Ciudadano. Fecha de corte: 31 de octubre de 2023

# Robo de Identidad

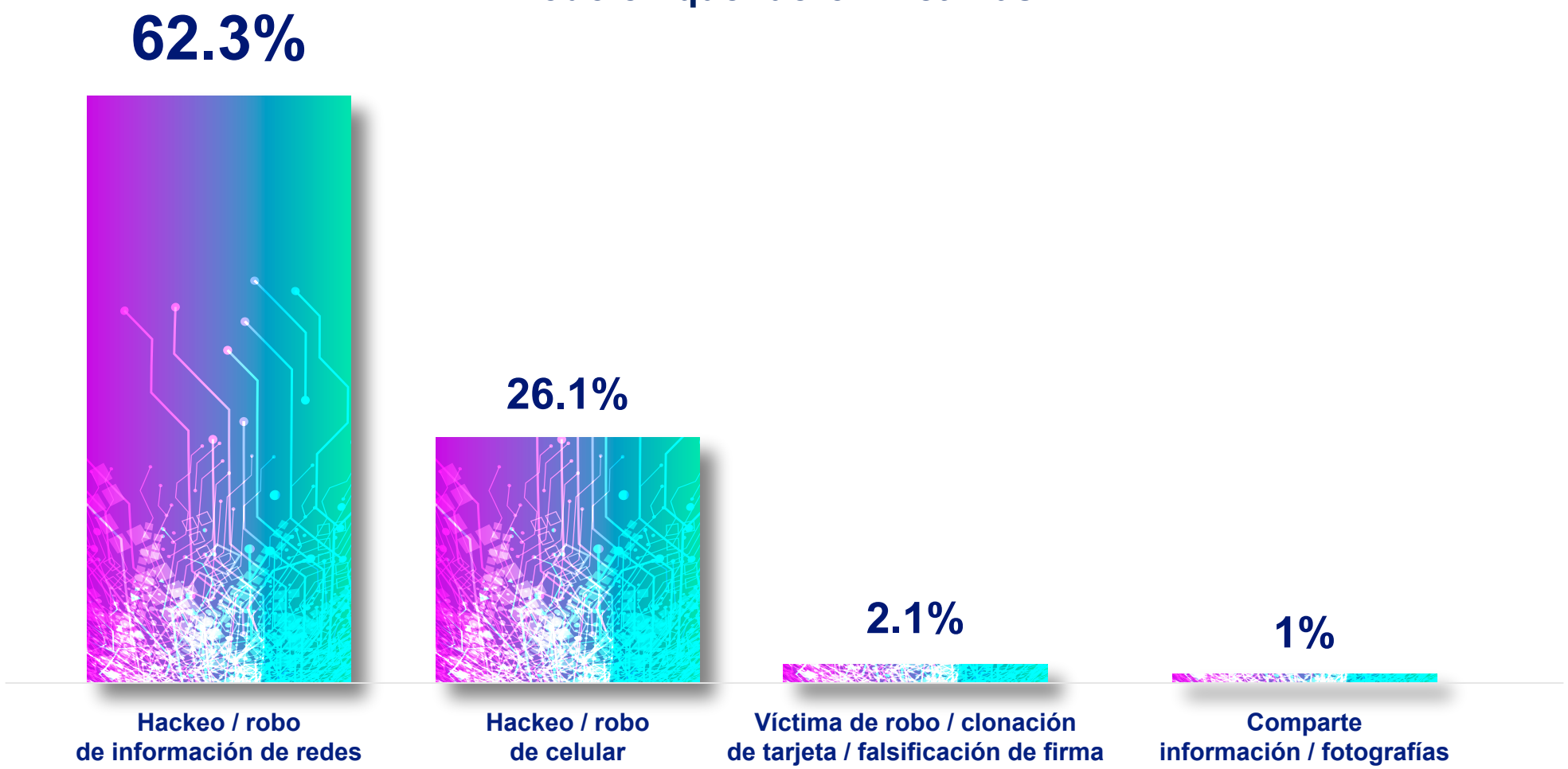
Durante enero-octubre de 2023 los reportes **aumentaron 218%** comparados con el mismo periodo de 2022.




Fuente: Consejo Ciudadano. Fecha de corte: 31 de octubre de 2023

# Robo de Identidad

## Modo en que fueron víctimas

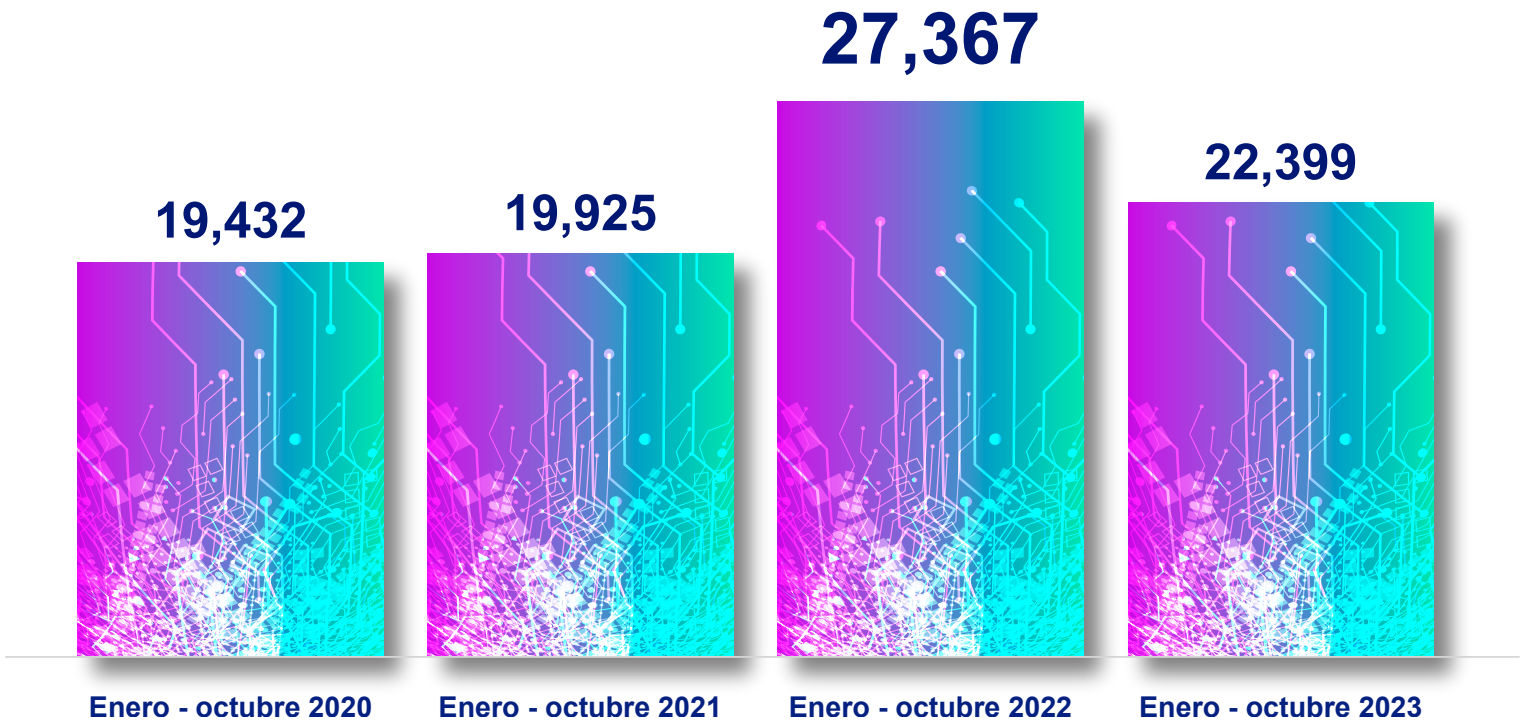



*El 8.3% de los reportes no especifica

Fuente: Consejo Ciudadano. Fecha de corte: 31 de octubre de 2023

# Extorsión

Los reportes por extorsión registran una **baja de 18%** entre 2022 y 2023.

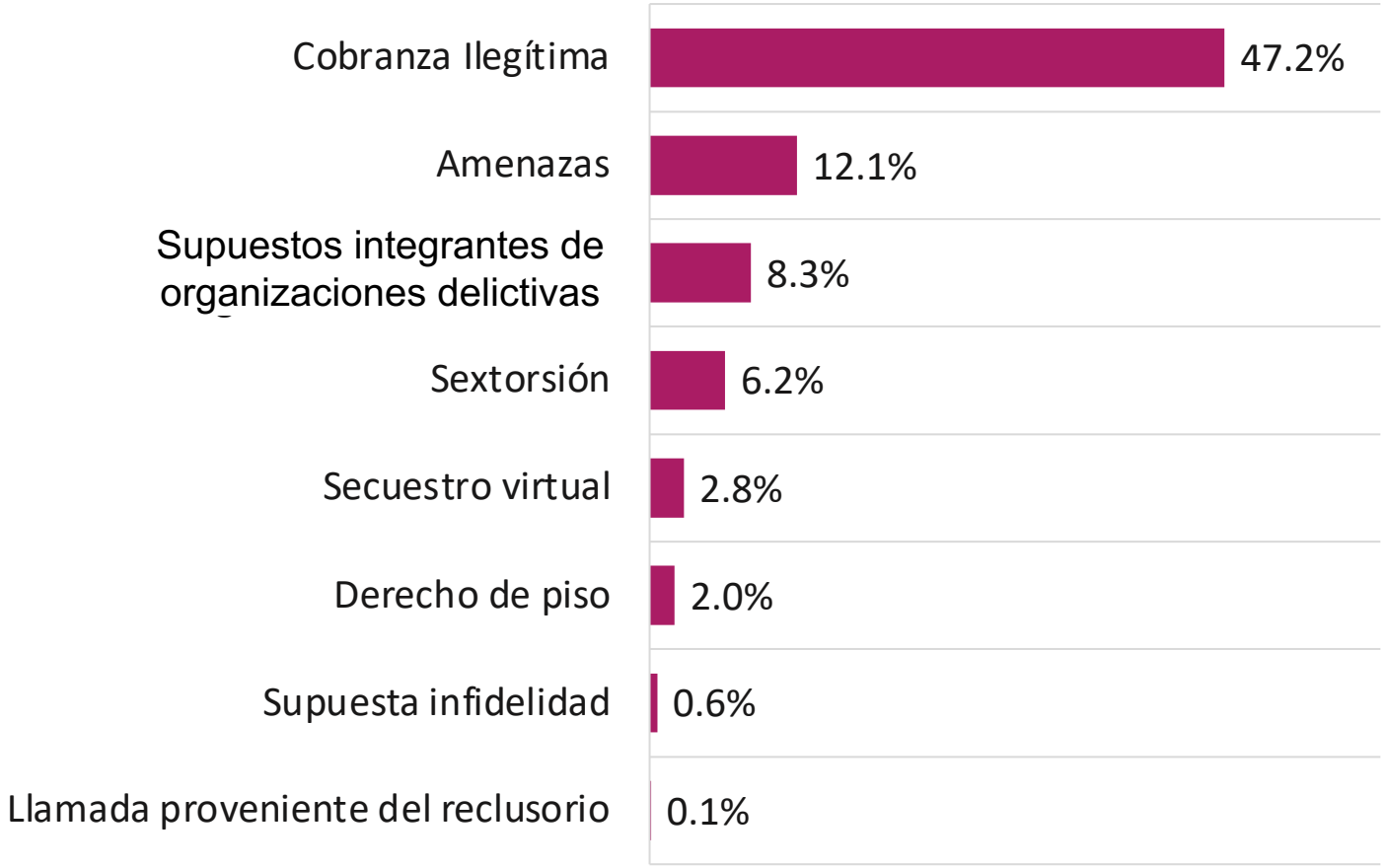



| Periodo | Totales | Promedio mensual |
|---|---|---|
| 2019 | 28,459 | 2,372 |
| 2020 | 23,868 | 1,989 |
| 2021 | 24,760 | 2,063 |
| 2022 | 31,438 | 2,620 |
| Enero-octubre 2023 | 22,399 | 2,240 |

Fuente: Consejo Ciudadano. Fecha de corte: 31 de octubre de 2023

# Modalidades extorsión

El **98% de las extorsiones se cometen vía telefónica**, que aumenta el riesgo ante la IA.




Tentativo
75%

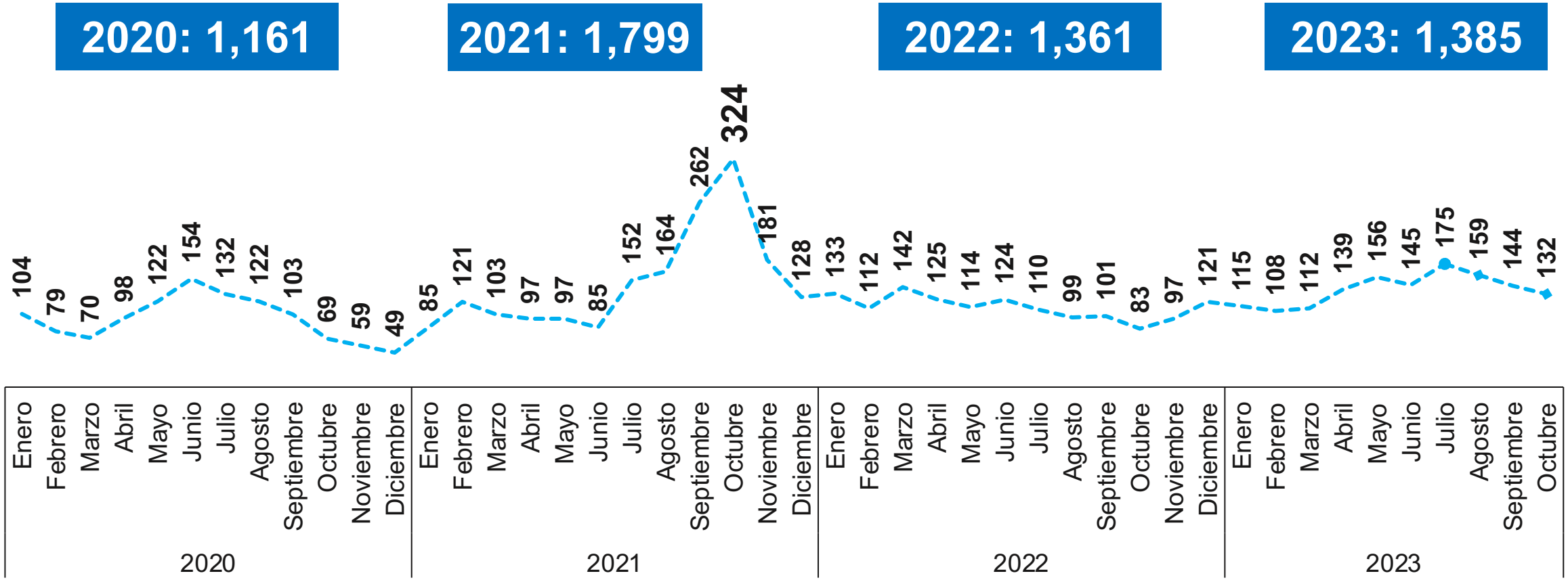
Consumado
25%

El 20.6% de las llamadas de extorsión pertenecen a llamadas de sondeo para recabar información de posibles víctimas (Bancos, seguros, etc.)

Fuente: Consejo Ciudadano. Fecha de corte: 31 de octubre de 2023

# Sextorsión

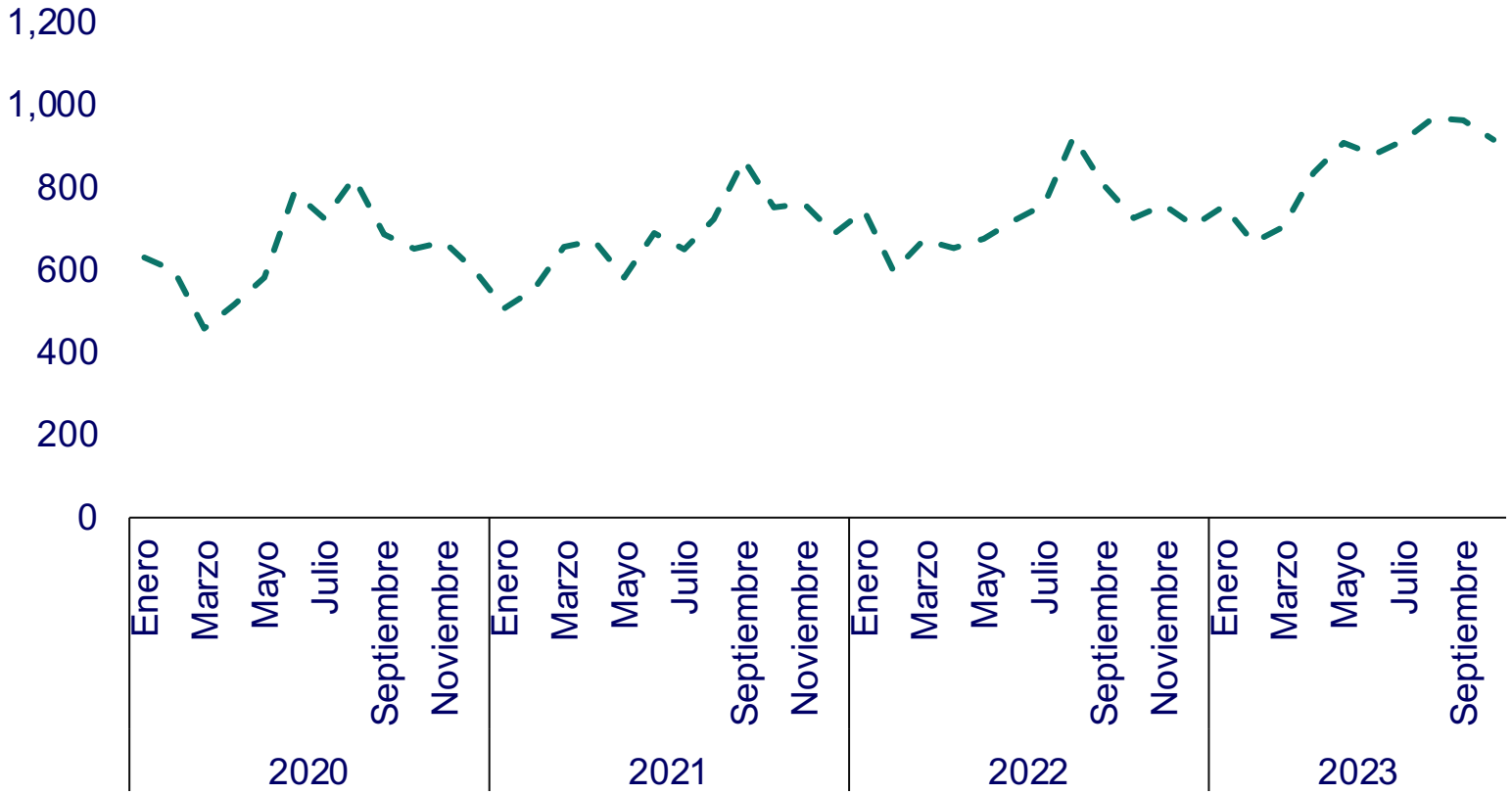
Por medio de la IA se pueden **alterar imágenes con contenido sexual** para extorsionar o venderlas como reales en medios digitales.

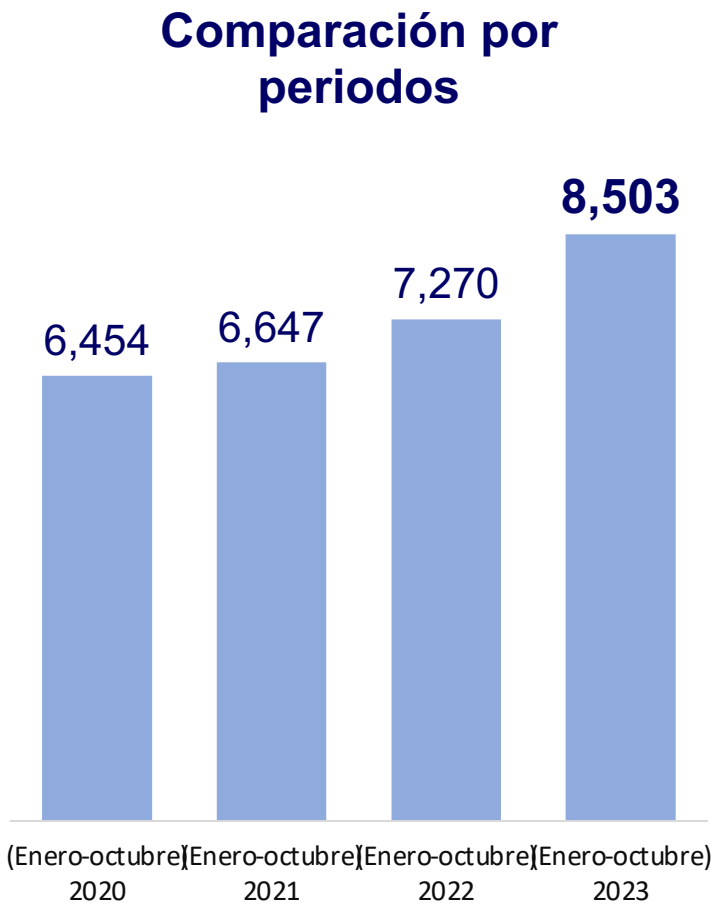



Fuente: Consejo Ciudadano. Fecha de corte: 31 de octubre 2023.

# Fraude

Durante 2023 **han incrementado los reportes un 17%** comparado con 2022.

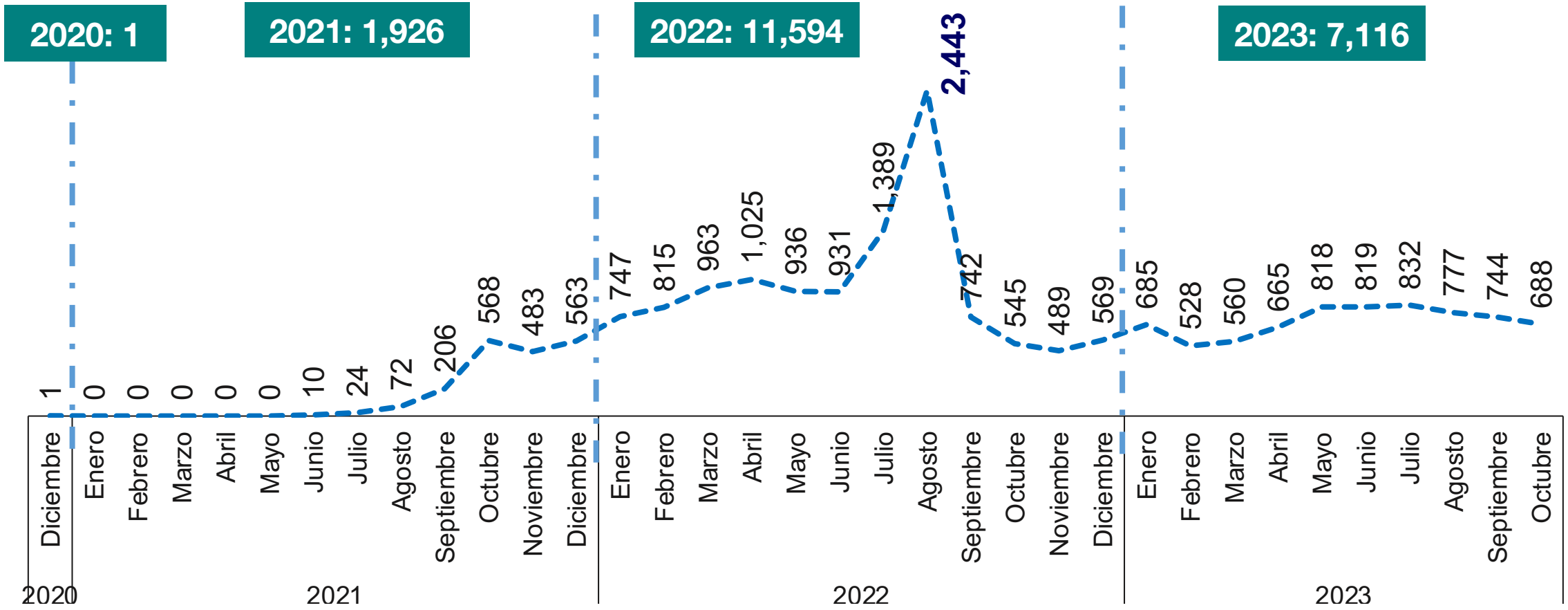



Fuente: Consejo Ciudadano. Fecha de corte: 31 de octubre de 2023

# Montadeudas

La IA puede ser **empleada por montadeudas para la cobranza ilegítima**, con falsos mensajes de sus víctimas o la recreación de situaciones.

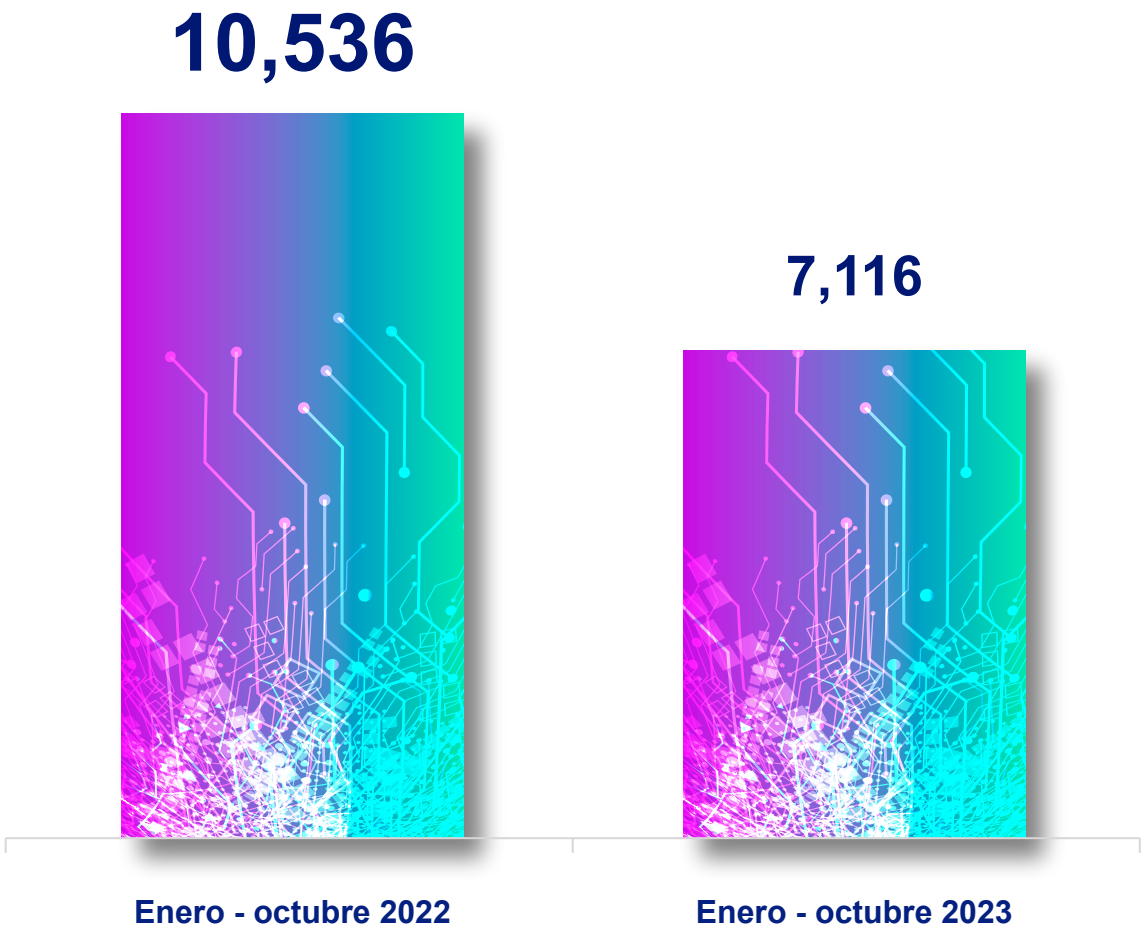



Fuente: Consejo Ciudadano Fecha de corte: 31de octubre de 2023

# Montadeudas

Durante 2023 han **disminuido los reportes 32%** en comparación al mismo periodo de 2022.

| Periodo | Reportes | Promedio mensual | Promedio diario |
|---|---|---|---|
| 2021 | 1,926 | 275 | 9 |
| 2022 | 11,594 | 966 | 32 |
| (Enero- octubre) 2023 | 7,116 | 712 | 23 |




Fuente: Consejo Ciudadano Fecha de corte: 31 de octubre de 2023

# Recomendaciones

Los quebrantos informativos son una mina de oportunidades delictivas, sean accidentales, por deslealtades o descuidos o provocados desde grupos de ataques locales o globales.

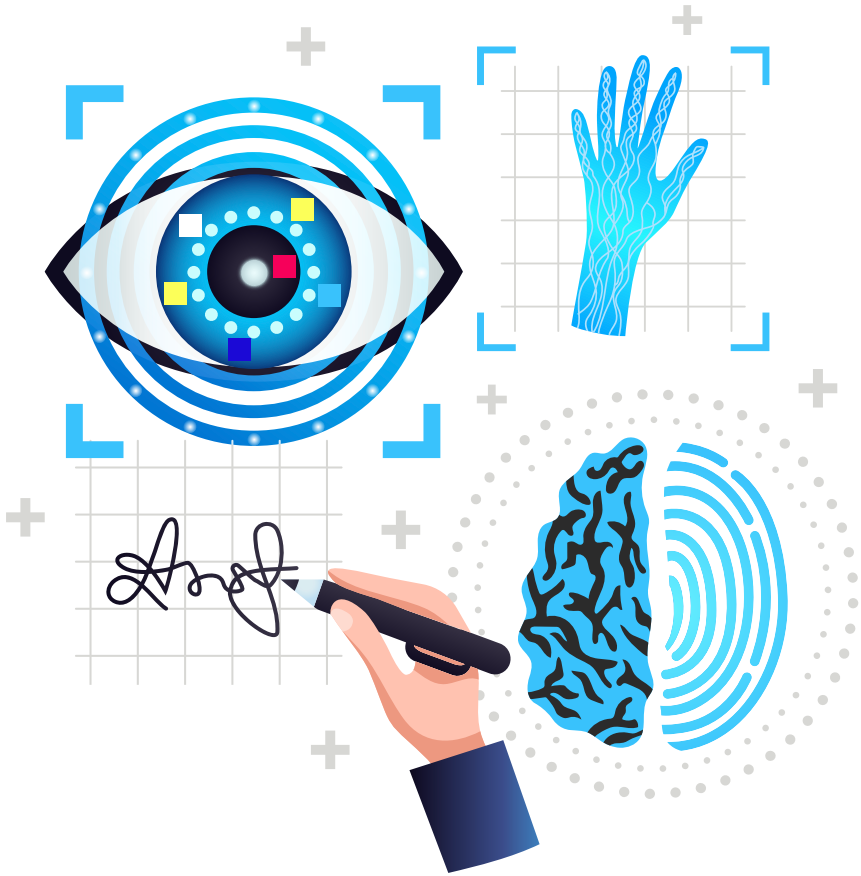
Ante estas circunstancias es necesario:

- **Ser conscientes de la amenaza**.

- Establecer **doble o múltiple autentificación** en dispositivos personales, corporativos o gubernamentales.

# Recomendaciones

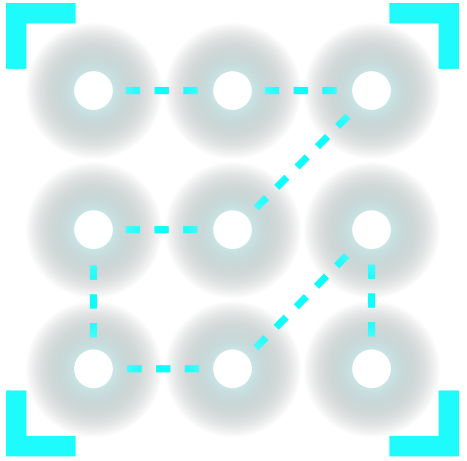
- **Crear y renovar passwords** y nombres de usuario, que sean robustos.
- Apartarse de correos o mensajes no deseados, no solicitados o de procedencia desconocida.
- Aplicar **configuraciones de privacidad** en redes sociales para limitar la exposición pública de fotos, videos y otra información personal.



# Recomendaciones

- Antes de compartir material comprobar la fuente de información.

- Aprender a **detectar deepfakes**:
  - ✓ En internet hay software de detección, como Sensity y RealityDefender, ambas de pago, o las gratuitas DeepfakeProof o Deepware.
  - ✓ Buscar en los videos señales como movimientos faciales inusuales o inconsistencias en el audio o video, cambios de iluminación de un fotograma al siguiente o en el tono de la piel, parpadeo extraño o ausencia del mismo.



# Recomendaciones

- Si quieres corroborar si una imagen es real, usa la **búsqueda inversa**.
- Impulsar equipos institucionales, de procuración de justicia y marcos normativos más actualizados.

# Gracias

consejociudadanomx.org

@consejociudadanomx @ConsejoCiudadanoMx @elconsejomx @consejociudadanomx