# ESTADÍSTICAS DE 2024

**859.532** Total de denuncias recibidas en 2024

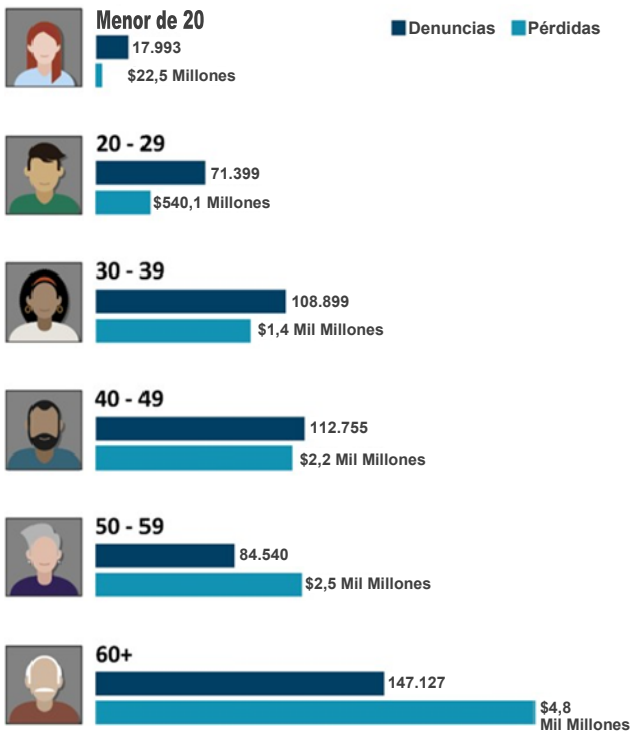
**$16,6 Mil Millones** Pérdidas en 2024

**33%** Aumento en pérdidas a partir de 2023

**256.256** Denuncias con pérdidas reales

**$16.372** Promedio de pérdidas

## Denuncias al IC3 agrupadas por edad




# ¡DENÚNCIELO!

Si existe la posibilidad de que usted o alguien que usted conoce sea víctima de fraude por Internet, presente una queja ante el IC3.

**www.ic3.gov**

Consejos para presentar denuncias:

- Conserve los documentos originales: correos electrónicos, cartas, cheques, recibos, documentos de envío, etc.
- Información de transacciones financieras.
- Información utilizada por los delincuentes tal como cuentas bancarias, direcciones, correos electrónicos, sitios web y números de teléfono.

Póngase en contacto con instituciones financieras para proteger sus cuentas y con las agencias de crédito para monitorear su identidad y detectar actividades sospechosas.

## Avisos de servicio al público y alertas para la industria

El IC3 revisa y analiza los datos presentados a través de su sitio web y genera productos de inteligencia para poner de relieve amenazas emergentes y nuevas tendencias. Los avisos de servicio al público, las alertas para la industria y otras publicaciones que describen estafas específicas se publican en el sitio web del IC3.

**www.ic3.gov**

**Departamento de Justicia de los EE. UU.**
Buró Federal de Investigaciones
*División de Cibernética*


# CENTRO DE DENUNCIAS DE DELITOS EN INTERNET

**www.ic3.gov**

# UN VISTAZO AL IC3

## La misión del IC3

La misión del Centro de Quejas de Delitos Cibernéticos (IC3) es proporcionar al público un medio seguro y conveniente para reportar información al Buró Federal de Investigaciones (FBI) sobre presuntas actividades delictivas facilitadas por Internet y para desarrollar alianzas eficaces con aliados en la industria. La información se procesa con fines de investigación e inteligencia para las autoridades y conocimiento del público

## Las denuncias al IC3

Las denuncias presentadas al IC3 abarcan una variedad de delitos por Internet, que incluyen el robo de derechos de propiedad intelectual, la intrusión informática, el espionaje económico, la extorsión en línea, y el lavado internacional de dinero. Entre los numerosos fraudes denunciados al IC3 se encuentran el robo de identidad, phishing, spam, reenvío, fraude por subastas, fraude de pagos, productos falsificados, estafas de romance, y estafa de no entrega de bienes.

## Fraude a personas de la tercera edad

La Ley de Prevención y Procesamiento del Abuso de Personas de la Tercera Edad se promulgó en octubre de 2017 para prevenir el abuso y la explotación de personas de la tercera edad, y mejorar la intervención del sistema de justicia en apoyo a las víctimas en casos de abuso y explotación de personas de la tercera edad. Como respuesta a la creciente prevalencia de fraude contra las personas de la tercera edad, el Departamento de Justicia (DOJ) y el FBI crearon la Iniciativa de Justicia para las Personas de la Tercera Edad. El Fraude de Personas de la Tercera Edad se define como una forma de fraude financiero dirigido o que afecta de manera desproporcionada a personas mayor de 60 años.

El IC3 es la oficina del FBI responsable de recibir las quejas de Fraude a Personas de la Tercera Edad. En 2024, más de 147.000 víctimas mayores de 60 años dieron parte al IC3 de pérdidas de $4,8 mil millones. Esto representa un aumento del 43 por ciento en pérdidas sobre las pérdidas reportadas en 2023. Debido a que la edad no es un dato requerido, estas estadísticas solo reflejan quejas en las que la víctima voluntariamente proporcionó su franja de edad como “Mayor de 60”.

## Los delitos por internet y el IC3

A medida que la tecnología evoluciona, también lo hacen los numerosos métodos utilizados para explotar la tecnología con fines delictivos. Casi todos los delitos que alguna vez se cometían en persona, por correo o por teléfono pueden ser cometidos por Internet. El elemento delictivo se ve empoderado por el anonimato percibido que ofrece el Internet y la facilidad de acceso a posibles víctimas. Los delincuentes utilizan la ingeniería social para aprovecharse de la simpatía, generosidad o vulnerabilidad de sus víctimas. El IC3 fue diseñado para ayudar a abordar todo tipo de delitos por Internet a través de su sistema de denuncias.

# TENDENCIAS

## Fraude de vulneración de correo electrónico empresarial

En 2024, el IC3 recibió 21.442 quejas de Vulneración de Correo Electrónico Empresarial (BEC) con pérdidas ajustadas de más de $2,7 mil millones. El BEC se dirige tanto a empresas como a individuos que realizan transferencias de fondos, y se lleva a cabo con mayor frecuencia cuando un sujeto compromete cuentas legítimas de correo electrónico empresarial a través de técnicas de ingeniería social o de intrusión informática para realizar transferencias no autorizadas.

## Estafa de confianza/romance

Las estafas de confianza/romance abarcan aquellas diseñadas para tocar las "fibras del corazón” de un individuo. En 2024, el IC3 recibió denuncias de 7.626 personas mayor de 60 años que experimentaron más de $389 millones en pérdidas por estafas de confianza/romance.

## Estafa de inversiones

El fraude de inversiones implica la venta ilegal o la supuesta venta de instrumentos financieros. Ejemplos de fraude de inversiones incluyen fraude de tarifas anticipadas, estafas piramidales y de Ponzi, estafas fraudulentas con criptomonedas, y fraude por manipulación del mercado. 47.919 víctimas reportaron estafas de inversiones en 2024, con pérdidas de más de $6,5 mil millones. De esas pérdidas, más de $5,8 mil millones correspondían a inversiones en criptomonedas. Las estafas de inversiones en criptomonedas vieron aumentos sin precedentes en el número de víctimas y pérdidas en dólares para estos inversores. Muchas víctimas han asumido deudas masivas para cubrir las pérdidas de estas inversiones fraudulentas y la franja de edad más señalada que denuncia este tipo de estafa comprende víctimas de 40 a 49 años.

## Programas de secuestro cibernético de datos (Ransomware)

El ransomware es un tipo de software malicioso, o malware, que cifra los datos en una computadora, haciéndola inutilizable. Un ciberdelincuente mantiene los datos como rehenes, o amenaza con destruir los datos o divulgarlos al público, hasta que se pague el rescate. Si no se paga el rescate, los datos de la víctima permanecen cifrados. En 2024, el IC3 recibió 3.156 quejas identificadas como ransomware con pérdidas ajustadas de más de $12,4 millones.

## Fraude de apoyo técnico y suplantación de gobierno

Las estafas de suplantación de identidad defraudan a miles de personas cada año. Dos categorías de fraude de reportadas a IC3, Apoyo Técnico/Atención al Cliente y Suplantación del Gobierno, son responsables de más de $1,8 mil millones en pérdidas. Los centros de llamadas se dirigen casi totalmente a los adultos mayores, con efectos devastadores. Casi la mitad de los demandantes informan ser mayor de 60 años (40%), y experimentan el 64% de las pérdidas (casi $1,2 mil millones).

## Criptomoneda

Antes limitada a hackers, grupos de ransomware y otros habitantes de la "web oscura", la criptomoneda se está convirtiendo en el método de pago preferido para todo tipo de estafas: intercambios de SIM, fraude de apoyo técnico, estafas de empleo, estafas de romance, incluso algunos fraudes de subastas.

El uso de criptomonedas en las estafas de inversión se propaga considerablemente, donde las pérdidas pueden alcanzar los cientos de miles de dólares por víctima. El IC3 recibió 149.686 quejas en 2024 a través de la cuales se denunció algún tipo de uso de criptomonedas. Las pérdidas implicadas en base a estas denuncias superaron los $9.3 mil millones.