



# BOLETÍN DE NOTICIAS DEL CONSUMIDOR DE LA FLORIDA

Abril 2025

Una Publicación del Departamento de  
Agricultura y Servicios al Consumidor

## ABRIL ES EL MES NACIONAL DEL CUIDADO DEL AUTOMÓVIL

Hay más de 18 millones de vehículos registrados en Florida, y esos vehículos representan una inversión significativa para los consumidores de Florida. Ocuparse de cualquier problema relacionado con el vehículo es importante para su seguridad y la longevidad de su vehículo. Sin embargo, es igualmente importante asegurarse de que el servicio y las reparaciones sean proporcionados por un taller de reparación de vehículos motorizados debidamente autorizado.

La Ley de Reparación de Vehículos Motorizados de Florida requiere que cualquier persona en Florida a quien se le pague por reparar vehículos motorizados propiedad de otras personas, se registre en el Departamento de Agricultura y Servicios al Consumidor de Florida (FDACS). Antes de contratar servicios con un taller de reparación de vehículos motorizados, use la función "Búsqueda de licencias comerciales" en [FloridaConsumerHelp.com](https://www.FloridaConsumerHelp.com) para garantizar que la empresa tenga la licencia adecuada.

Comience a buscar un taller de reparación antes de que lo necesite. Es más probable que tome una mejor decisión si no tiene prisa o entra en pánico. Cuando seleccione un negocio, asegúrese de que respeten la garantía de su vehículo, si corresponde. Siempre es una buena idea pedir recomendaciones a amigos y asociados.

Pregunte cómo se estiman los precios de la tienda antes de hacer arreglos para hacer cualquier reparación. Algunos talleres cobran una tarifa plana por la mano de obra en las reparaciones, mientras que otros pueden cobrar por la mano de obra según el tipo de trabajo realizado. Si el trabajo de reparación costará más de \$150, el taller de reparación DEBE darle la opción de solicitar un presupuesto por escrito, ser notificado por el taller si la reparación excede una cantidad que usted especifique, o no requerir un presupuesto por escrito en absoluto. Los talleres de reparación de vehículos motorizados no pueden obligarlo a renunciar a su derecho a un presupuesto.

No elija un taller de reparación de vehículos motorizados solo porque ofrecen la reparación menos costosa. Ahorrar unos pocos dólares y no reparar su vehículo correctamente puede terminar costándole más a largo plazo. Si no está seguro de necesitar una reparación específica, no tenga miedo de obtener una segunda opinión.

El Departamento de Agricultura y Servicios al Consumidor de Florida es el centro de intercambio de información del estado para las quejas, la protección y la información de los consumidores. Si necesita presentar una queja sobre un taller de reparación de vehículos motorizados, comuníquese con el Centro de Asistencia al Consumidor de FDACS al 1-800-HELP-FLA (435-7352) o, para hispanohablantes, 1-800-FL-AYUDA (352-9832) o visite [File a Complaint](https://www.FloridaConsumerHelp.com). Para obtener más información sobre los talleres de reparación de vehículos motorizados, visite [Consumer Rights and Responsibilities/Motor Vehicle Repair](https://www.FloridaConsumerHelp.com) en [FloridaConsumerHelp.com](https://www.FloridaConsumerHelp.com).



[www.FloridaConsumerHelp.com](https://www.FloridaConsumerHelp.com)

1-800-HELP-FLA(435-7352) • Mon-Fri, 8a.m. – 5p.m., EST • 1-800-FL-AYUDA(352-9832)

# LAVADO DE CHEQUES

La Red de Ejecución de Delitos Financieros (FinCEN, por sus siglas en inglés), una oficina del Departamento del Tesoro de los Estados Unidos ha identificado el fraude con cheques como la mayor fuente de ganancias ilícitas en los Estados Unidos. Los informes de la Ley de Secreto Bancario por fraude con cheques han aumentado significativamente en los últimos años, y las instituciones financieras presentan más informes de actividades sospechosas (SAR) a FinCEN. La Ley de Secreto Bancario de 1970, también conocida como Ley de Información de Divisas y Transacciones Extranjeras, es una ley estadounidense que exige a las instituciones financieras de los Estados Unidos que ayuden a las agencias gubernamentales de los Estados Unidos a detectar y prevenir el lavado de dinero.

A pesar de la disminución del uso de cheques en los Estados Unidos, los delincuentes se han dirigido cada vez más al correo de los EE. UU. para cometer fraudes con cheques desde la pandemia de COVID-19. Los delincuentes que cometen este tipo de fraude de cheques relacionado con el robo de correo generalmente roban cheques personales, cheques comerciales, cheques de reembolso de impuestos y cheques relacionados con programas de asistencia gubernamental, como pagos del Seguro Social y beneficios de desempleo.

El Servicio de Inspección Postal de los Estados Unidos (USPIS, por sus siglas en inglés) ha informado que el fraude de cheques relacionado con el robo de correo es cada vez más cometido por estafadores que van desde estafadores individuales hasta grupos delictivos organizados compuestos por los organizadores del esquema criminal, reclutadores, lavadores de cheques y mulas de dinero. Estos delincuentes se dirigen a las cajas azules de recolección de USPS, los buzones residenciales no seguros y las unidades de cajas agrupadas de propiedad privada en complejos de apartamentos, vecindarios planificados y edificios comerciales de alta densidad.

**Mula de Dinero:** una persona (ya sea consciente o inconscientemente) que transfiere o mueve fondos ilícitos bajo la dirección o en nombre de otra.

Los estafadores alteran o “lavan” los cheques, reemplazando la información del beneficiario con sus propias identidades o identidades fraudulentas o con cuentas comerciales que los delincuentes controlan. A menudo aumentarán el monto en dólares del cheque, a veces en cientos o miles de dólares. Los cheques lavados también pueden copiarse, imprimirse y venderse a estafadores externos en la web oscura y plataformas de redes sociales encriptadas a cambio de moneda virtual convertible. En algunos casos, los cheques de las víctimas también se falsifican utilizando la información de ruta y cuenta del cheque original robado.

**Lavado de Cheques:** el uso de productos químicos para eliminar la tinta original de un cheque para reemplazar al beneficiario y, a menudo, el monto en dólares. Los estafadores también pueden copiar e imprimir varios cheques lavados para usarlos en el futuro o para venderlos a terceros delincuentes.

En muchos casos, los delincuentes pueden cobrar o depositar cheques en persona en instituciones financieras, a través de cajeros automáticos (ATM) o mediante depósito remoto en cuentas que controlan, y que a menudo abren específicamente para los esquemas de fraude con cheques. También pueden utilizar mulas de dinero y sus cuentas pre-existentes para depositar cheques fraudulentos. De todos modos, una vez que se depositan los cheques, los estafadores a menudo retiran rápidamente los fondos a través de cajeros automáticos o los transfieren a otras cuentas que controlan para complicar aún más el rastro del dinero. Después del robo inicial y la negociación fraudulenta de los cheques robados, los delincuentes pueden continuar explotando a sus víctimas utilizando la información de identificación personal que se encuentra en el correo robado para futuros esquemas de fraude, como el fraude con tarjetas de crédito o el fraude de cuentas de crédito.



# LAVADO DE CHEQUES: PROTÉJASE

Los inspectores postales recuperan más de \$1 mil millones en cheques falsos y giros postales cada año, pero usted puede tomar medidas para protegerse.

- **Use bolígrafos de tinta de gel negro indelebles cuando escriba cheques.** Debido a sus propiedades químicas, la tinta indeleble puede resistir la mezcla de lavado típica de un estafador, que puede incluir acetona, lejía y alcohol isopropílico.
- **Utilice comprobaciones con una o más características de seguridad.** Los fabricantes de cheques agregan sellos distintivos específicos a los cheques para reducir las posibilidades de fraude. Hable con su banco para confirmar que sus cheques tienen algunas de estas características, como marcas de agua, pantógrafos de copia nula, tinta de seguridad, fibras visibles o invisibles, holobanda reflectante tridimensional y microimpresión de alta resolución.
- **No pongas cheques en el buzón de tu casa para que los recojas.** La banderita que alerta a su cartero también puede indicar a los posibles ladrones que hay algo dentro.
- **Deposite el correo antes de la última recogida.** Evite dejar cheques en cajas azules de cobro durante la noche, ya que son más vulnerables a los robos.
- **Recupere el correo con frecuencia.** Nunca deje su correo en su buzón durante la noche.
- **Mantenga el correo en la oficina de correos.** Si se va de vacaciones, haga que su correo lo guarde en la oficina de correos o que lo recoja un vecino, amigo o familiar.
- **Use métodos de pago electrónicos:** Siempre que sea posible, opte por el pago electrónico de facturas o transferencias en lugar de enviar cheques por correo.
- **Monitoree su cuenta bancaria en línea con regularidad.** Confirme los cheques que se han cobrado y reporte cualquier cosa que parezca sospechosa.
- **Reporte cualquier actividad sospechosa a su banco:** Si sospecha que sus cheques han sido robados o alterados, repórtelo a su banco de inmediato.

Si cree que ha sido víctima de un fraude de cheques relacionado con el robo de correo, comuníquese de inmediato con su institución financiera y repórtelo al USPS al [1-877-876-2455](tel:1-877-876-2455) o <https://www.uspis.gov/report>.



# CUIDADO CON LA FATIGA DE MFA

La autenticación multifactorial (MFA) es una medida de seguridad crucial que proporciona una capa adicional de protección a sus cuentas. Incluso si un ciberdelincuente logra robar su nombre de usuario y contraseña, MFA hace que sea significativamente más difícil para ellos obtener acceso. Desafortunadamente, los ciberdelinquentes han desarrollado tácticas para manipular a las personas para que aprueben solicitudes de inicio de sesión maliciosas.

La fatiga de MFA, también conocida como bombardeo de MFA o agotamiento de MFA, es un ciberataque que consiste en enviar solicitudes repetidas de MFA a una víctima. El objetivo es engañar a la víctima para que apruebe una solicitud, lo que le daría al atacante acceso a la cuenta de la víctima. Al enviar avisos repetidos de MFA, los ciberdelinquentes pueden aprovechar cuando las personas se distraen, se frustran o aprueban por error un aviso de MFA fraudulento. Cuando esto sucede, el atacante puede comprometer la capa adicional de seguridad y obtener acceso a su cuenta.

Su concienciación es la primera y mejor línea de defensa contra las amenazas cibernéticas. ¡PIENSA SIEMPRE ANTES DE HACER CLIC! Mantenga sus cuentas seguras al no aprobar nunca las siguientes indicaciones de MFA...

- **Avisos inesperados de MFA:** Avisos que aparecen mientras ya está conectado a una cuenta o en un momento inusual o avisos que no inició. Si recibe un mensaje de MFA inesperado, considérela sospechoso y no lo apruebe.
- **Avisos de MFA que aparecen después de abrir un mensaje sospechoso:** Si recientemente recibió un correo electrónico de phishing o hizo clic en un enlace que solicitaba sus credenciales, ¡no apruebe la solicitud de MFA! ¡Restablezca su contraseña y repórtelo de inmediato!
- **Varias solicitudes de MFA seguidas:** si recibe varias solicitudes de MFA consecutivas, es posible que un atacante que utilice la táctica de fatiga de MFA no las apruebe.
- **Solicitud de MFA desde ubicaciones o dispositivos desconocidos:** si recibe una solicitud de MFA desde una ubicación o un dispositivo desconocidos (no la apruebe), los intentos legítimos de inicio de sesión se originan en su dispositivo y ubicación.
- **Llamadas telefónicas o mensajes de texto pidiéndole que apruebe un aviso de MFA:** Los estafadores que se hacen pasar por el soporte de TI pueden llamar y pedirle que apruebe un aviso de MFA. No apruebe el mensaje, restablezca su contraseña e infórmelo de inmediato.
- **Páginas de inicio de sesión desconocidas:** no introduzcas las credenciales de tu cuenta en páginas de inicio de sesión desconocidas, no autorizadas o inesperadas.

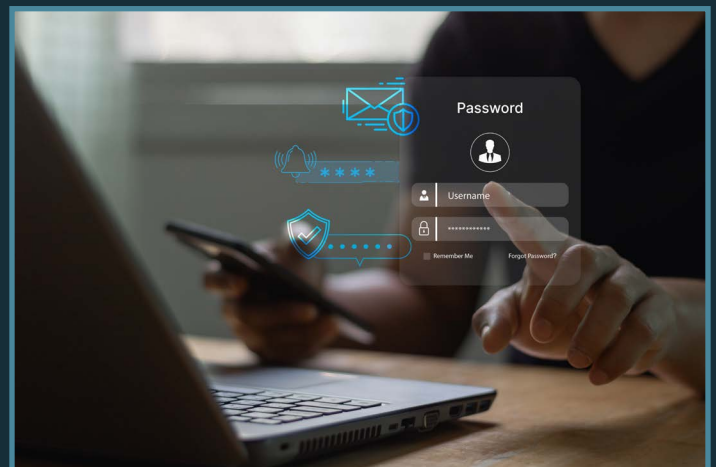
**Consejo Profesional:** Si experimenta solicitudes de MFA frecuentes y no autorizadas, habilite la coincidencia de números o la autenticación biométrica en lugar de las notificaciones automáticas para mejorar la seguridad.

La coincidencia de números es una configuración que te obliga a introducir números de la plataforma de identidad en tu aplicación para aprobar una solicitud de autenticación. El requisito de coincidencia de números mitiga la fatiga de MFA al:

- Requerir acceso a la pantalla de inicio de sesión para aprobar solicitudes. Los usuarios no pueden aprobar solicitudes sin ingresar los números en la pantalla de inicio de sesión.
- Desalentar el spam de avisos. Cada solicitud genera un conjunto único de números para cada solicitud de inicio de sesión. Como el usuario no puede aceptar las solicitudes sin conocer los números, la generación de varias solicitudes no es eficaz.

La autenticación biométrica se refiere a un proceso de ciberseguridad que verifica su identidad utilizando sus rasgos biológicos únicos, como huellas dactilares, voces, retinas y rasgos faciales.

**Denunciar mensajes de correo electrónico sospechosos:** Si reconoce un correo electrónico como spam o sospecha que es malicioso, reenvíelo a [reportphishing@apwg.org](mailto:reportphishing@apwg.org) (una dirección utilizada por el Grupo de Trabajo Antiphishing, que incluye ISP, proveedores de seguridad, instituciones financieras y agencias de aplicación de la ley). Informe a la empresa o persona que se hizo suplantación sobre el esquema de phishing y repórtelo a la Comisión Federal de Comercio en [FTC.gov/Complaint](https://www.ftc.gov/complaint).



# ESTAFA DE PREMIOS

Por el Personal de la FTC

Los estafadores a veces te hacen pensar que has tenido un golpe de buena suerte. Pero si su carta de premio en efectivo de un millón de dólares viene con instrucciones para pagar una pequeña tarifa, tal vez por impuestos, informes o manejo, no es suerte. Es una estafa. Si pagas, perderás tu dinero y descubrirás que no hay premio. ¿Puedes detectar una estafa de premios?

Los estafadores utilizan la promesa de un premio para robar su dinero o su información personal. Es posible que digan que son de una empresa conocida como Publishers Clearing House y te llamen, envíen un mensaje de texto, te envíen un correo electrónico o un mensaje en las redes sociales para decirte que eres elegible para el dinero del premio. Pero te dirán que primero debes enviarles dinero, tal vez para pagar una tarifa para liberar el dinero no reclamado, por ejemplo. Ninguna empresa real te hará pagar para reclamar un premio. Solo un estafador lo hará. Antes de responder, reduzca la velocidad y hágase estas preguntas:



Congratualtions!  
You've won a \$1,000 gift card.  
Go to <http://youwon/456789>  
to claim now.



- **¿Qué dicen los demás?** Busque en línea y vea lo que encuentra sobre el concurso o la empresa. Escribe el nombre con términos como “revisión”, “queja” o “estafa”.
- **¿Alguien más recibió este mensaje?** Mientras revisas en línea, fíjate si otras personas informan haber recibido el mismo mensaje. Si recibiste la oferta por correo, mira el matasellos en el sobre o la tarjeta postal. Una tarifa al por mayor significa que otras personas recibieron la misma oferta.
- **¿Me pidieron que pagara o que diera información personal confidencial?** Si es así, es una estafa. No hay ninguna razón para dar su cuenta bancaria o número de Seguro Social para reclamar un premio. Y solo un estafador insistirá en que pague transfiriendo dinero a través de una empresa como Western Union o MoneyGram, usando una aplicación de pago como Apple Pay, CashApp, PayPal o Zelle, enviando dinero en efectivo o pagando con tarjetas de regalo o criptomonedas para obtener su premio.

Comparta esta alerta con familiares y amigos para ayudarlos a evitar también las estafas de premios. Si detecta uno, dígaselo a la FTC al [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud). Visitar [Prize and Grant Scams](#) para obtener más información.

# ACERCA DE LA DIVISIÓN FDACS DE SERVICIOS AL CONSUMIDOR

FDACS es la agencia estatal de protección al consumidor de Florida responsable de manejar las quejas de los consumidores y regular muchas industrias que afectan directamente a los consumidores de Florida. FDACS maneja más de 400,000 quejas y consultas de los consumidores, supervisa más de 500,000 dispositivos regulados, entidades y productos como bombas de gas y básculas de comestibles, realiza más de \$30,000 análisis de laboratorio en productos como gasolina y fluido de freno, realiza casi 9,000 inspecciones de paseo justo y devuelve más de \$2.8 millones a los consumidores a través de mediaciones con empresas.



La División de Seguridad Alimentaria supervisa los alimentos desde el punto de fabricación y distribución a través de las ventas al por mayor y al por menor para garantizar al público productos alimenticios seguros, saludables y debidamente representados.

**OPRIMA EN EL ICONO ANTERIOR PARA VER LO RETIRADO, LOS RETIROS DEL MERCADO Y LAS ALERTAS DE SEGURIDAD**



La Comisión de Seguridad de Productos de Consumo proporciona información sobre la retirada de productos de consumo como parte de la misión de la agencia de proteger a los consumidores y a las familias de los productos peligrosos.

**OPRIMA EN EL ICONO ANTERIOR PARA VER LO RETIRADO, LOS RETIROS DEL MERCADO Y LAS ALERTAS DE SEGURIDAD.**

El Departamento de Agricultura y Servicios al Consumidor de Florida es el centro de intercambio de información del estado para quejas, protección e información de los consumidores. Los consumidores que deseen información sobre la presentación de una queja contra una empresa o que crean que se ha producido fraude pueden visitarnos en línea en [FloridaConsumerHelp.com](http://FloridaConsumerHelp.com) o ponerse en contacto con la línea directa de información y protección al consumidor del departamento llamando al 1-800-HELP-FLA (435-7352) o al 1-800-FL-AYUDA (352-9832) en español.