



BOLETÍN DE NOTICIAS DEL CONSUMIDOR DE LA FLORIDA

Enero 2026

Una Publicación del Departamento de
Agricultura y Servicios al Consumidor

AÑO NUEVO, NUEVA MEMBRESÍA EN EL GIMNASIO

¡Feliz Año Nuevo! Si acaba de empezar el camino hacia una versión más saludable de sí mismo gracias a una resolución que ha tomado, ¡enhorabuena! Si está decidido/decidida a encontrar el lugar perfecto para entrenar, siga leyendo para descubrir cómo puede protegerse en lo que respecta a la suscripción al gimnasio.

Apuntarse a un gimnasio suena fácil y algunos incluso ofrecen pruebas gratuitas. Sin embargo, el Better Business Bureau advierte que no comparta la información de su cuenta bancaria o tarjeta de crédito cuando se inscribas en esa prueba gratuita. Muchos gimnasios empezarán a cobrar automáticamente una cuota de membresía si olvida cancelar su “suscripción”. Asegúrese de entender todos los términos y condiciones de la prueba gratuita y de que cualquier compromiso termine en un plazo determinado.

Imagina que has encontrado el gimnasio perfecto y firmado el contrato, pero luego decides que no es el lugar para ti. Pensabas que cancelar sería fácil: solo tienes que conectarte a internet y seleccionar “cancelar”. El proceso no es tan sencillo en algunos gimnasios; De hecho, podría ser bastante complicado cancelarlo. Por ejemplo, la Comisión Federal de Comercio alega que LA Fitness hizo casi imposible que sus clientes cancelaran su contrato, lo que suponía un exceso de tiempo y dinero para quienes querían salir.

Se anima a los consumidores a investigar antes de elegir un gimnasio para asegurarse de que no haya problemas cuando llegue el momento de dejar la membresía

- **Consulte las opiniones en línea.** Busque el nombre del gimnasio y la palabra “suscripción” o “contrato”, además de palabras como “reclamación”, “problema”, “cancelación” y “cuota”. Lea los resultados para hacerse una idea de lo fácil o difícil que es terminar una relación con el gimnasio.
- **Lea la letra pequeña.** Todos sabemos que hay que hacer esto al comprar una casa, un coche u otro artículo importante, pero puede que no pensemos que se aplica a la suscripción al gimnasio. ¡Desde luego que sí! ¿La membresía se renueva automáticamente? ¿Cómo se le notifica de los cambios de precio? ¿Qué tiene que hacer para cancelar?
- **Haga preguntas.** Haga que el personal le explique qué está incluido en la membresía y qué no. Pregunte específicamente sobre renovaciones y cancelaciones.

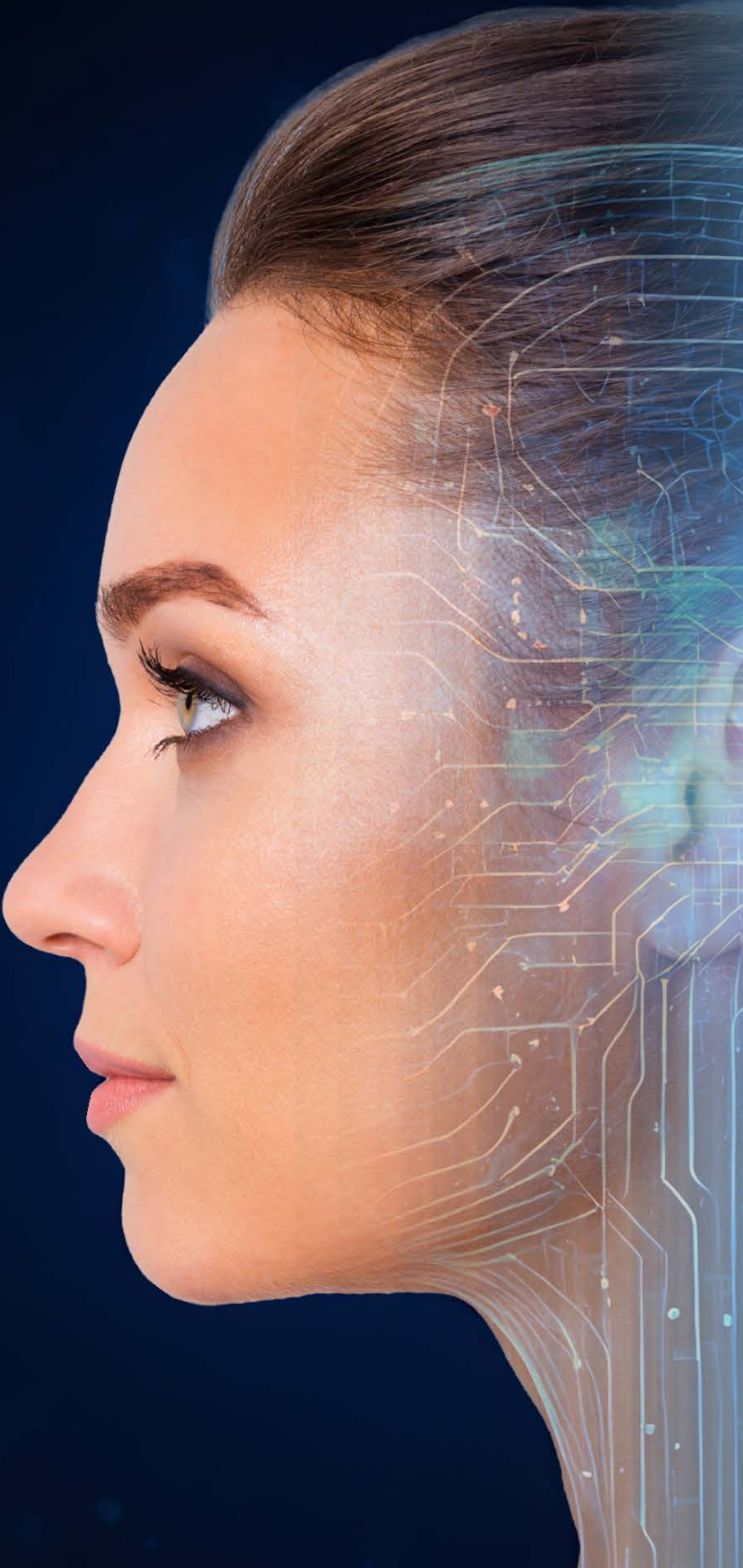
Si ya tiene membresía y ha intentado cancelar, pero solo siguen cobrando tu tarjeta, contacta con tu banco para disputar los cargos y bloquear cargos futuros. Es seguro que su contrato será cancelado rápidamente.

Según la Ley de Estudios de Salud de Florida, los estudios de salud (gimnasios) están obligados a registrarse en el Departamento de Agricultura y Servicios al Consumidor de Florida (FDACS). Además, algunos estudios de salud deben instalar seguridad durante un tiempo limitado. Al exigir a los estudios de salud que proporcionen una fianza u otra seguridad financiera, el FDACS puede proporcionar cierta protección financiera a los miembros de un estudio de salud que cierre inesperadamente. Los fondos pueden luego utilizarse para compensar a los miembros que compren contratos a largo plazo. Lee más sobre tus derechos y cómo protegerte en nuestra [página web](#). Para asegurarse de que el gimnasio que elija está registrado, visita [Búsqueda de Empresas](#). Si tiene una queja sobre un estudio de salud, utiliza nuestro [formulario de reclamaciones en línea](#) o llama al 1-800-HELP-FLA (435-7352).

www.FloridaConsumerHelp.com

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

¿ESE VÍDEO ES REAL O NO? DEEPFAKE (VIDEOS FALSOS)



En nuestra discusión continua sobre inteligencia artificial, o IA, este mes abordaremos vídeos creados con inteligencia artificial. Estos vídeos se conocen comúnmente como deepfakes; La definición de deepfakes (vídeos falsos) incluye imágenes o sonidos en los que el rostro, cuerpo o voz de una persona han sido alterados digitalmente y a menudo se usan de forma maliciosa o para difundir información falsa. Según una investigación de la empresa de identidad digital Signicat, los deepfakes han aumentado más de un 2.100% desde que la IA generativa se popularizó en 2022. Para los fines de este artículo, cubriremos vídeos deepfake.

EJEMPLOS DE VÍDEOS DEEPFAKE (FALSOS)

¿Recuerdas cuándo la prueba en vídeo era una prueba irrefutable de lo que se mostraba en el vídeo? Las pruebas en vídeo ya no pueden usarse como pruebas independientes debido a deepfakes; Los vídeos son de apoyo, junto con el testimonio de testigos y otras pruebas que lo acompañan. Existen muchas formas de vídeos deepfake, como se indica en la lista de abajo y cómo se pueden utilizar.

Deepfakes con intercambio de caras: Estos vídeos superponen el rostro de una persona sobre el cuerpo de otro cuerpo en movimiento. Las redes neuronales de IA son hábiles para emparejar expresiones cuadro a cuadro con el cuerpo en movimiento, creando un vídeo realista. Algunos de estos deepfakes son solo por diversión, pero otros pueden usarse con fines maliciosos, como arruinar una reputación o difundir información falsa.

Sincronización labial y superposiciones de audio: A veces llamado puppeteering (marioneta), los deepfakes con sincronización labial reorganizan los movimientos de la boca para que coincidan con el audio, que puede ser manipulado o completamente sintetizado. Combinado con la clonación de voz, que cubrimos el mes pasado, la “persona” del vídeo parece hablar, pero las palabras nunca fueron pronunciadas por nadie.

Recreación de cuerpo completo: Estos vídeos presentan modelos generados completamente por IA, que capturan la postura, los gestos y los movimientos de un actor, y los atribuyen a otra persona. Estos deepfakes presentan a una persona o personas que parecen estar realizando tareas o participando en actividades que nunca han hecho. Aunque las películas y la televisión utilizan esto en el rodaje, el uso malévolo es el de pruebas montadas y vídeos falsos de coartadas.

ESTAFAS CON VÍDEOS DEEPFAKE

Estafas de inversión: Estate atento a las solicitudes de inversión de tus estrellas favoritas. Los estafadores crean vídeos deepfake, utilizando la imagen de gurús financieros o celebridades que animan a los espectadores a invertir en esquemas falsos o acuerdos “exclusivos”. Después de enviar el dinero o de proporcionar la información personal, el estafador ya no puede ser localizado, sin que la víctima pueda devolver. Un ejemplo es una estafa reciente que involucra al “CEO” de una empresa cripto. Un vídeo que recluta inversionistas con el “CEO” era en realidad un avatar recitando un guion, todo programado con IA.

Estafas románticas: Tenga cuidado al buscar una relación online. Si conoces a alguien que parece encantador y demasiado bueno para ser verdad, puede que lo sea. Tras crear cuentas falsas, el estafador utiliza IA para generar fotos, vídeos e incluso videollamadas que pueden ser deepfakes para construir relaciones. Tras ganarse la confianza de su víctima, el estafador comienza a pedir dinero o información financiera personal.

Fraude: Los estafadores están utilizando deepfakes de IA para cometer fraude en redes sociales. Al manipular vídeos y audio de creadores de contenido, crean contenido nuevo que parece ser el creador original vendiendo un producto (inexistente) por una causa (falsa). Los vídeos deepfake están dirigidos a los seguidores o audiencia del creador.

Entre las celebridades más con videos falsos está Taylor Swift, que “apareció” en una serie de anuncios en redes sociales ofreciendo utensilios de cocina Le Creuset gratis. Los participantes solo tenían que proporcionar su información personal y pagar el envío. Desgraciadamente, los vídeos eran falsos y ella nunca hizo tal oferta. Los estafadores se llevaron la información financiera y personal de miles de Swifties, además del dinero.

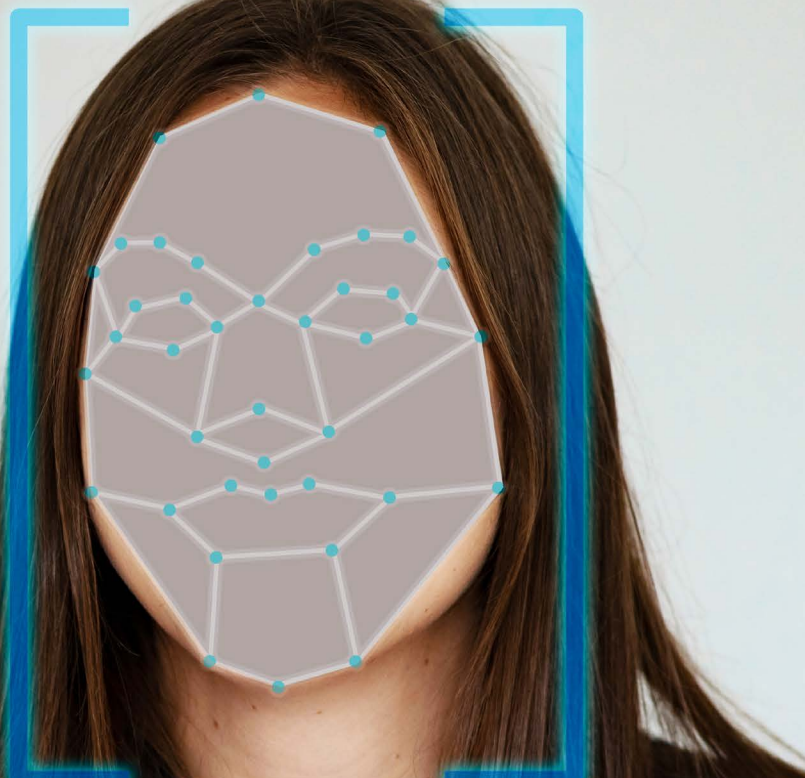
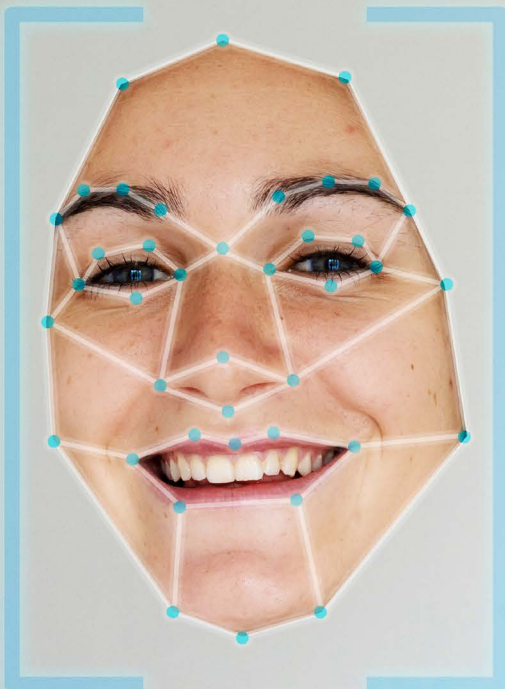
DETECCIÓN DE DEEPFAKES

¿Cómo puedes tú, el profano, determinar si un vídeo es un deepfake? Aquí tienes algunos ejemplos que puedes emplear sin tener que comprar equipos digitales extensos.

Observación humana: Tu primera línea de defensa para determinar si un vídeo es un deepfake es observar detenidamente. Busca pistas de que la figura del vídeo es una ilusión, como acciones antinaturales, rasgos faciales en los que la expresión está desajustada o distorsionada, y movimientos inconsistentes. ¿El pelo y los dientes parecen reales? ¿Son naturales los movimientos oculares? Presta atención a las sutiles anomalías en la textura de la piel, patrones parpadeantes o reflejos desajustados.

Pistas contextuales: Considera el fondo del vídeo. ¿No hay sombras cuando debería haberlas? ¿O las sombras no son consistentes con la iluminación? Fíjate si el audio y el vídeo están desincronizados. Si hay objetos moviéndose, ¿tiene sentido el movimiento?

Referenciar la fuente: Si ves un vídeo sospechoso que indique la presencia de alguien, consulta la fuente oficial de la ubicación para probar o refutar la afirmación. Las notas de prensa suelen contener ángulos de cámara alternativos para demostrar tales afirmaciones. Los medios de comunicación convencionales dependen de estos controles cruzados en nombre de la credibilidad.



ESTAFAS DE SECUESTRO

El 5 de diciembre de 2025, la Oficina Federal de Investigaciones (FBI) emitió un [anuncio](#) advirtiendo al público sobre estafadores que encuentran y alteran fotos encontradas en sitios web y redes sociales para usarlas en estafas virtuales de secuestro. Estos malos actores simulan un secuestro falso y luego exigen un rescate.

Contacto del “Secuestrador”

Los delincuentes involucrados en esta estafa suelen contactar con sus víctimas enviando un mensaje de texto, también conocido como smishing, afirmando haber secuestrado a un familiar o ser querido para extorsionar dinero a la víctima. En este intercambio de mensajes, el “secuestrador” amenazará con actos violentos significativos si no se cumplen inmediatamente las demandas de rescate y continúa con fotos o videos del ser querido. Estas fotos están programadas para que la víctima no tenga tiempo de examinarlas y confirmar su autenticidad. Al observarlas detenidamente, las imágenes pueden tener proporciones extrañas o pueden faltar detalles verificables, como cicatrices o tatuajes. Las fotos originales han sido modificadas para encajar en la narrativa del estafador, por lo que podría ser una foto familiar, recortada, con un fondo añadido u otros detalles.

Protéjase

- Acordaos una palabra clave que solo tú y tus seres queridos conozcáis para verificar la comunicación.
- Comparte fotos de tu familia y de ti solo con quienes conoces, no con el público. La configuración de privacidad de Facebook te permite limitar quién puede ver tus publicaciones e información de perfil.
- Cuando viajes, no proporciones información personal a desconocidos y espera a volver a casa para publicar esas preciosas fotos de vacaciones.
- Si publicas información sobre personas desaparecidas en internet, ten cuidado con la información que te proporcionan desconocidos, ya que podría ser una estafa.

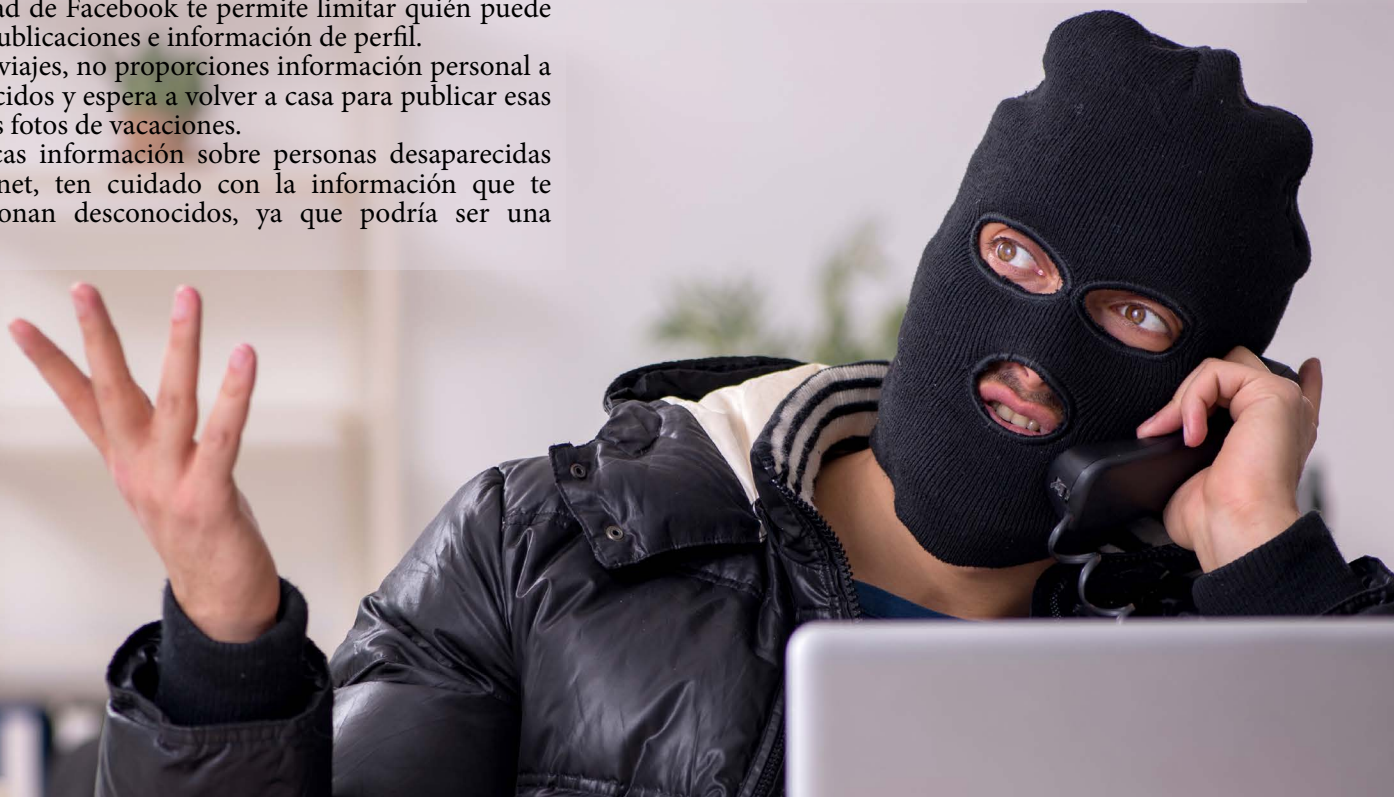
Si recibes un mensaje diciendo que un ser querido ha sido secuestrado y exigiendo un rescate,

- No reacciones ante una falsa sensación de urgencia. Tómate el tiempo para procesar lo que está pasando.
- Considera la afirmación del secuestrador: ¿tiene sentido?
- Haz capturas de pantalla o graba fotos de pruebas de vida siempre que sea posible.
- Intenta siempre contactar con tu ser querido antes de plantearte pagar el rescate.

En una segunda advertencia el 8 de diciembre, el FBI volvió a advertir al público sobre el peligro de estafas. “Si te sientes presionado a actuar rápido, pagar dinero o entregar información personal—tómate un respiro. Para y evalúa si lo que te dicen es real. Hablad con vuestras familias. Protegernos mutuamente de las estafas”, dijo el director del FBI, Kash Patel. “Los estafadores apuestan a que te vas a sentir demasiado avergonzado para denunciar el crimen al FBI. No dejes que ganen.”

Denúncialo

Si eres víctima de una estafa de secuestro virtual, denuncia el incidente al Centro de Denuncias de Delitos en Internet del [FBI en www.ic3.gov](https://www.ic3.gov). Asegúrate de enviar toda la información posible sobre la interacción, incluyendo números de teléfono, datos de pago, mensajes de texto y audio, y fotos de prueba de vida. Llevar un registro de toda la información es útil en una investigación.



UTILIZA ESTE PLAN DE ACCIÓN PARA EVITAR ESTAFAS

Los estafadores [cuentan muchas historias diferentes](#) para intentar conseguir tu dinero o tu información personal. Podrían mentir y decir que le debes dinero al gobierno. O finge ser tu banco y di que te han hackeado la cuenta. Podrían alegar que alguien de tu familia tuvo una emergencia o que tu ordenador tiene un virus. O podrían decir otra mentira.

Los estafadores te cuentan todas estas cosas para intentar que entres en pánico. Quieren que te des prisa y hagas lo que te dicen antes de que tengas tiempo de pensar, leer su historia o contactar con alguien que pueda intervenir.

Ahí es donde la nueva herramienta de la FTC, [Cómo evitaré una estafa: mi plan de acción](#), puede ayudar. Puedes usarlo para hacer una lista de personas en las que confías — quizá tu amigo, vecino, padre, hija o nieto — a quienes puedas acudir si crees que podrías estar tratando con un estafador. Hablarlo puede ayudarte a darte cuenta de que algo no va bien.

El Plan de Acción también te permite incluir la información de contacto de las empresas con las que haces negocios — como tu compañía de tarjetas de crédito, tu banco y tus sitios de compras online favoritos— para que sepas cómo contactarlas directamente si te preocupa que haya algún problema con tu cuenta.

Las estafas pueden afectar a cualquiera en cualquier momento. Así que [haz tu propio plan de acción](#). Publícala en la nevera o guárdala cerca del móvil o del ordenador. Luego ayuda a otros en tu vida a crear uno:

- Compártalo con sus hijos, padres o abuelos
- Compártalo con sus compañeros, amigos y vecinos
- Compártalo en su iglesia, biblioteca local o centro comunitario

Pide ejemplares gratis para compartir [aquí](#). Y como siempre, si detectas una estafa, avisa a la FTC: [ReportFraud.ftc.gov](https://www.ftc.gov/whistleblower).



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 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.