



# BOLETÍN DE NOTICIAS DEL CONSUMIDOR DE LA FLORIDA

April 2026

Una Publicación del Departamento de  
Agricultura y Servicios al Consumidor

## LO QUE NECESITA SABER SOBRE LAS CRIPTOMONEDAS

La criptomoneda (cripto) se lanzó públicamente por primera vez en 2009, en forma de Bitcoin. Desde entonces, se han introducido más de 25.000 criptomonedas más, y la forma de moneda digital sigue atrayendo atención. ¿Qué es exactamente la criptomoneda? ¿Cómo se utiliza? Sigue leyendo para descubrir los datos básicos sobre este activo digital.

**¿Qué pasa?** La criptomoneda es una moneda virtual garantizada por criptografía (o código) y no depende de una autoridad central, como un banco, para mantenerla. Los registros de propiedad y transacciones se almacenan en un formato de base de datos denominado bloque. Los registros, o bloques, se enlazan de uno a otro mediante un hash (o identificador único) para formar una cadena y se distribuyen a través de una red de ordenadores peer-to-peer, a menudo pública. Los bloques enlazados se llaman blockchain. Los datos dentro de cualquiera de los bloques no pueden cambiarse sin modificar los datos de bloques posteriores, lo que requeriría permiso en toda la red. Dado que la blockchain es descentralizada y de código abierto, las transacciones se registran en toda la red, son verificables en tiempo real y pueden auditarse de forma económica. No hay tiempo muerto esperando a que una transacción se “compense”, ni temor a falsificaciones.

**¿Es moneda física?** Las criptomonedas existen en forma de moneda o token. Los tokens son activos intangibles en una blockchain, mientras que las monedas pueden ser tangibles, virtuales o digitales. Bitcoin fue el primero en introducirse y es el más comúnmente negociado. Otras criptomonedas, denominadas altcoins, son Ethereum, Litecoin y Solana, entre miles de otras. Todos estos se clasifican según su función y tecnología respectivas; Hay monedas de pago para transacciones, tokens de utilidad para contratos inteligentes o acceso a plataformas, y stablecoins vinculadas a activos, así como categorías menos utilizadas como monedas de privacidad o meme.

**¿Cómo se adquiere?** Las criptomonedas pueden comprarse y venderse en un intercambio de criptomonedas, donde intercambias moneda física (dólares y centavos) por unidades de moneda virtual almacenadas en una cartera digital. Una cartera digital puede ser hardware, software o un servicio que almacena tus claves públicas y privadas para transacciones digitales. Las claves privadas se utilizan para autorizar gastos y las claves públicas para aceptar fondos.

**¿Qué puede comprar con ella?** Las monedas de pago en criptomonedas pueden usarse en numerosos comercios online para comprar una gran variedad de productos, desde artículos de reparación en el hogar hasta bienes raíces, incluyendo tarjetas regalo que luego pueden usarse en el comerciante designado.



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

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

**¿Cómo está respaldado?** Las monedas fiduciarias, como el dólar estadounidense o los euros, están respaldadas por la fortaleza de la economía más que por una materia prima física como el oro. Sin embargo, las criptomonedas están respaldadas por la seguridad de la blockchain, la rareza de la moneda, la descentralización (o la facilidad de validación de las transacciones) y la eficacia.

**¿Se tributa la criptomoneda?** El IRS considera que las criptomonedas son propiedad y están sujetas al impuesto sobre ganancias de capital.

**¿Es seguro el cripto?** Como se compra y vende en internet, las criptomonedas conllevan los riesgos habituales de las compras online. Cuando compres, infórmate bien. Considera la seguridad, la facilidad de uso, los activos en manos y las comisiones al seleccionar un intercambio. Valora también tus opciones con carteras digitales. Las carteras calientes, que están conectadas a internet, pueden permitir un comercio más rápido y más comodidad, pero son más vulnerables a hackeos, phishing y malware. Sin embargo, las carteras frías almacenan tu cripto fuera de línea en un dispositivo físico de almacenamiento digital, ofreciendo así un mayor grado de seguridad. Sin embargo, ten cuidado con no perder el dispositivo o dañarlo, porque podrías perder permanentemente los fondos almacenados en él.

**¿Reflexiones finales?** Decidir una inversión requiere un pensamiento cuidadoso y planificación. Invertir en criptomonedas no es diferente. Sigue investigando tus opciones y, basándote en tus hallazgos, puedes invertir con confianza siempre que tomes decisiones acertadas:

1. elegir un método de almacenamiento;
2. investiga monedas antes de comprar;
3. utilizar una bolsa de confianza confiable; y
4. Sigue siempre las normas habituales de ciberseguridad.

#### Referencias

Datos sobre blockchain de Investopedia (s.d.): qué es, cómo funciona y cómo puede utilizarse. Recuperado de [Blockchain Facts: ¿Qué es?, cómo funciona y cómo se puede utilizar](#)

Charles Schwab (2025) ¿Qué es la criptomoneda y cómo funciona? Recuperado de [¿Qué es la criptomoneda y cómo funciona? \(2025\) | Charles Schwab](#)

El Tonto Heterogéneo (2025) ¿Qué es el almacenamiento en frío en las criptomonedas? Recuperado de [¿Qué es el almacenamiento en frío en cripto? | El Loco, Heterogéneo](#)

Fidelity (2025) Cómo almacenar criptomonedas de forma segura y recuperarlas de [¿Es seguro bitcoin? | Cómo comprar y almacenar criptomonedas de forma segura](#)



# INTERCAMBIO DE SIM: LA ESTAFA QUE PUEDE SECUESTRAR TUS CUENTAS BANCARIAS

Imagina despertarte una mañana y descubrir que tu teléfono de repente no tiene cobertura. No hay llamadas. Sin mensajes. Sin datos.

Al principio, puede parecer una simple caída de servicio o un fallo de red. Sin embargo, en cuestión de horas, tus cuentas bancarias, perfiles en redes sociales, cuentas de correo electrónico e incluso fondos de jubilación podrían ser tomados por delincuentes.

Aunque tu teléfono físico siga en tus manos, los estafadores pueden robar algo mucho más valioso: el control de tu número de teléfono. Este número suele ser la clave para verificar tu identidad en banca online, servicios de pago y otras cuentas.



## **Dato rápido**

*Según el Centro de Denuncias por Delitos en Internet del FBI, las estafas de intercambio de SIM causaron casi 26 millones de dólares en pérdidas reportadas en Estados Unidos en 2024, y el número de víctimas sigue creciendo cada año.*

Estas estafas permiten a los delincuentes interceptar los códigos utilizados para acceder a tus cuentas financieras y online.

## **Cómo funciona la estafa**

Los delincuentes suelen utilizar dos métodos para controlar el número de teléfono de una víctima: el intercambio de SIM y el fraude por portabilidad.

## **Intercambio de SIM**

Una tarjeta SIM es un pequeño chip dentro de tu teléfono que almacena el ID único de tu cuenta y vincula tu número con tu cuenta móvil. En un ataque de intercambio de SIM, estafadores engañan al operador móvil para que active una nueva tarjeta SIM vinculada a tu número de teléfono, transfiriendo efectivamente tu número a un dispositivo que controlan.

Muchos proveedores están cambiando ahora a tarjetas SIM integradas (eSIM), que están integradas directamente en el dispositivo y no pueden ser retiradas. Aunque esta tecnología reduce ciertos riesgos, los estafadores pueden intentar apoderarse de cuentas engañando a las operadoras para que crean que la solicitud de transferencia de número de teléfono proviene del titular legítimo de la cuenta, un proceso conocido como ingeniería social.

## **Estafas de portabilidad**

Una estafa de portabilidad ocurre cuando un delincuente transfiere fraudulentamente tu número de teléfono a otro proveedor móvil. Normalmente, portar tu número es un proceso legítimo al cambiar de operador o actualizar dispositivos.

Sin embargo, los estafadores pueden recopilar información personal sobre una víctima y hacerse pasar por ella al solicitar la transferencia. Una vez completada, el delincuente recibe todas las llamadas y mensajes de texto dirigidos a la víctima, incluidos los códigos de autenticación de dos pasos (2FA) y los mensajes de restablecimiento de contraseña.

Con acceso a estos códigos, los delincuentes pueden:

- Accede a cuentas bancarias y transfiere fondos
- Solicita crédito o préstamos a nombre de la víctima
- Secuestro de cuentas en redes sociales

## Cómo Protegerte

### 1. Añade un PIN de Seguridad a Su Cuenta Móvil

La mayoría de los operadores permiten a los clientes colocar un PIN de salida de portabilidad o transferencia SIM. Esto añade un paso adicional de verificación para evitar transferencias no autorizadas.

### 2. Utilice aplicaciones de autenticación en lugar de códigos de texto

Siempre que sea posible, utiliza aplicaciones de autenticación, biometría o tokens de seguridad en lugar de verificación por SMS. Estos métodos son más seguros contra el intercambio de SIM.

### 3. Limitar la información personal en línea

Los estafadores suelen recopilar información de las redes sociales para hacerse pasar por víctimas. Mantén la información personal privada siempre que sea posible.

### 4. Vigila los mensajes de phishing

No proporciones información personal si alguien llama, correo o envía mensajes pidiéndola. Si la persona que llama dice representar a una empresa, cuelga y contacta directamente con la empresa usando un número de teléfono de confianza.

### 5. Manténgase Alerta

Activa alertas por correo electrónico y SMS para cuentas financieras e importantes. Contacta inmediatamente con tu banco o proveedor si detectas alguna actividad sospechosa.

### 6. Actúa rápido si tu teléfono pierde el servicio

Muchos ataques de SIM swap ocurren tarde por la noche mientras las víctimas duermen. Si tu teléfono pierde el servicio de repente sin explicación:

- Contacta inmediatamente con tu operadora móvil
- Notifique a sus entidades financieras
- Usa Wi-Fi o el móvil de un amigo para actuar rápido

Cada minuto cuenta, ya que los estafadores pueden intentar acceder a cuentas en cuestión de horas.

Tu teléfono ya no es solo una forma de hacer llamadas, forma parte de tu **identidad digital**. Proteger tu número de teléfono es tan importante como proteger tu cartera, tus contraseñas y tu futuro financiero.

## Referencias

Comisión Federal de Comunicaciones. (s.f.). Fraude telefónico. Recuperado de

<https://www.fcc.gov/consumers/guides/cell-phone-fraud>

Comisión Federal de Comunicaciones. (s.f.). El fraude por portabilidad apunta a tus cuentas privadas. Recuperado de

<https://www.fcc.gov/consumers/guides/port-out-fraud>

Oficina Federal de Investigaciones. (2025). Centro de Denuncias por Delitos en Internet (IC3) Informe de Delitos en Internet 2024. Recuperado de

[https://www.ic3.gov/Media/PDF/AnnualReport/2024\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf)



# RECUPERAR BIENES ROBADOS DE UNA CASA DE EMPEÑOS

Imagina que sufres un robo en casa y que los objetos son robados incluyen herramientas costosas y joyas heredadas. El robo fue denunciado y usted proporcionó una descripción detallada de todo lo que faltaba. Luego descubres que parte de tu propiedad se vendió en una casa de empeños local. Te sientes aliviado de que tus bienes hayan sido recuperados... ¿O no? ¿Te lo devolverán todo? Sigue leyendo para descubrir qué tienes que hacer para recuperar tu propiedad.

Las sentencias judiciales de Florida han dictaminado que las fuerzas del orden no pueden recuperar bienes robados de una casa de empeños y devolverlos al propietario, ya que al prestamista se le permite la oportunidad de una audiencia. ¿Qué significa esto para ti, como propietario de la propiedad? Hay dos opciones: puedes optar por comprar tu propiedad al prestamista u obtener una orden judicial para que te devuelvan la propiedad sin coste adicional.



La [Ley de Empeño de Florida](#), sección 539.001, Estatutos de Florida, detalla los pasos que deben seguirse para recuperar sus objetos robados mediante orden judicial. Primero, el prestamista debe ser notificado de tu intención de recuperar los objetos. Este aviso debe incluir:

- el nombre y la dirección de la casa de empeño;
- tu nombre completo y número de teléfono;
- una descripción completa y precisa del(los) artículo(s), incluyendo números de serie, si procede;
- una copia del informe del robo de la agencia policial; y,
- Una afirmación similar a la siguiente:

*La agencia de seguridad (nombre de la agencia) ha determinado, a lo largo de una investigación penal, que en la siguiente fecha (fecha de empeño), mis bienes personales robados fueron empeñados en tu negocio. El número de control del slip de peón es: (número de control). Mis bienes personales fueron empeñados por (inserta nombre Y apellido del vendedor). He incluido una copia del informe policial con este aviso. Quiero que me devuelvan los artículos SIN COSTE.*

El aviso debe estar firmado y fechado por usted, el propietario de la propiedad, y entregado en mano para que sea firmado y fechado por un empleado de la casa de empeños, o entregado por correo certificado, con acuse de recibo. (Puedes descargar una versión rellenable del aviso [aquí](#).)

Si no has llegado a un acuerdo con el prestamista en los diez días siguientes a la recepción de la notificación, tendrás que solicitar al tribunal una audiencia, nombrando al prestamista como demandado y perfeccionando la notificación, ambos aspectos sin coste para ti, ya que la tasa judicial y la tasa por servicio del sheriff están exentas por ley.

Si el tribunal determina que la propiedad debe ser devuelta, puede recuperar todos los costes de la acción del prestamista, incluidos los honorarios del abogado.

Todas las casas de empeño en Florida están obligadas a solicitar y obtener una licencia cada año del Departamento de Agricultura y Servicios al Consumidor de Florida (FDACS). Cada casa de empeño debe mantener un patrimonio neto de al menos 50.000 dólares o presentar una garantía en forma de fianza, carta de crédito o certificado de depósito por un importe de 10.000 dólares. La FDACS está autorizada a imponer sanciones de hasta 5.000 dólares por incumplimiento de la ley. Para más información sobre casas de empeño, visita nuestra [página web](#).

# FRAUDE EN MEDICARE

En septiembre de 2025, el Departamento de Justicia de EE. UU. (DOJ) anunció la acusación formal de dos hombres de Florida acusados de defraudar Medicare por valor de 34,8 millones de dólares. Más tarde, en diciembre, dos ejecutivos sanitarios fueron condenados por estafar otros 34 millones de dólares de Medicare Advantage. A continuación, un propietario de laboratorio de Lake Worth fue condenado por perpetrar un esquema de fraude de Medicare valorado en 52 millones de dólares. Eso supone más de 120 millones de dólares en fondos públicos perdidos en Florida y eso es solo lo que se ha descubierto. Titulares aún más recientes revelan cientos de millones de dólares en reclamaciones falsas de hospicio en California. Cada una de estas situaciones implicaba facturar a Medicare por equipos, recetas, pruebas o servicios innecesarios y solo se descubrieron tras la pérdida de millones de dólares. Sin embargo, existen formas en que los inscritos en Medicare y sus cuidadores pueden ayudar a detener este fraude antes.

Las historias anteriores acaban de salir a la luz en los últimos seis meses y representan un problema generalizado. El fraude en Medicare cuesta a los contribuyentes estadounidenses 60.000 millones de dólares cada año y sus efectos son preocupantes. No solo desperdicia dinero de los contribuyentes, sino que también puede causar problemas a los inscritos en Medicare. La información médica falsa puede resultar en una atención sanitaria inadecuada o incluso en la denegación de servicios que se necesitan y merecen.

A continuación, se muestran las formas en que los inscritos en Medicare o sus cuidadores pueden vigilar y detectar fraudes, reportando los problemas lo antes posible.

- Habla con el médico. En cuanto al tratamiento y el coste, los inscritos tienen derecho a saber exactamente qué costes se facturarán a Medicare.
- Lleva buenos registros. Documenta todos los servicios recibidos, incluyendo fechas, tipo de servicios y la condición que se trató. Guarda cualquier extracto que se proporcione en la cita, especialmente si incluye códigos de facturación; Si no se lo proporciona, pide uno.
- Revisa el correo. O, mejor aún, revisa la cuenta online. Crea una cuenta en <https://www.medicare.gov/account/login> y supervisa tu cuenta siempre que tengas una cita o recibas bienes o servicios. Los extractos con la misma información se envían periódicamente a los inscritos.
  - o Los Avisos Resumen de Medicare (MSN) se envían dos veces al año. El MSN proporciona un resumen de todas las reclamaciones presentadas durante el mes anterior y cuánto se pagó.
  - o Una Explicación de Beneficios (EOB) es similar a un MSN y se envía mensualmente a los inscritos en Medicare Advantage.



Revisa la cuenta o extracto para asegurarte de que fechas, códigos de facturación e importes coinciden. Si el extracto incluye el nombre de un médico no atendido, tratamiento o equipo no recibido, o servicios no prestados, contacte con el proveedor de facturación, que debe informar del error a Medicare, y la cuenta se actualizará. Si el proveedor no lo informa, contacte con Medicare.

- No facilites el número de Medicare del beneficiario a nadie que no sea el proveedor, que incluye al médico o al centro médico.
- No aceptes servicios “gratuitos” a cambio del número del inscrito en Medicare.

Si se sospecha de fraude, llame al 1-800-MEDICARE (1-800-633-4227) o [informe del fraude de Medicare en línea](#). Participar activamente en su trayectoria sanitaria permite a los inscritos en Medicare comprender mejor sus condiciones y tratamiento, y ayuda a prevenir el fraude, lo que beneficia a todos.

## Referencias

Departamento de Justicia de EE. UU. 7 de septiembre de 2025. [Oficina de Asuntos Públicos | Dos hombres de Florida acusados de esquema de fraude de 34,8 millones de dólares dirigido a beneficiarios de Medicare | Departamento de Justicia de los Estados Unidos](#)

Departamento de Justicia de EE. UU. 7 de enero de 2026. [Distrito Sur de Florida | Dos ejecutivos sanitarios condenados por explotar beneficiarios de Medicare Advantage en un esquema de fraude de 34 millones de dólares | Departamento de Justicia de los Estados Unidos](#)

Departamento de Justicia de EE. UU. 29 de enero de 2026. [Distrito Sur de Florida | El propietario de un laboratorio en Florida se declara culpable de un esquema de fraude de Medicare de 52 millones de dólares relacionado con pruebas genéticas | Departamento de Justicia de los Estados Unidos](#)

CBS News. 10 de marzo de 2026. [Investigación de CBS News: Cientos de hospicios de Los Ángeles presentan múltiples indicadores de fraude](#)

Fox News. 12 de marzo de 2026. [Número de Medicare de un médico de 87 años vinculado a 600 millones de dólares en fraude | Fox News](#)

AARP. (sin fecha) [Ayuda a detener el fraude de Medicare](#)

Medicare (sin fecha) [Denunciar fraude y abuso de Medicare | Medicare](#)



# CÓMO EVITAR ESTAFAS AL SOLICITAR EL ESTA

De [Federal Trade Commission](#)

Es esa época del año en la que la gente empieza a planificar sus viajes de primavera y verano. Si tienes a alguien que te visita desde otro país (y califica para una [exención de visado](#)), tendrá que completar una solicitud [de Sistema Electrónico de Autorización de Viaje \(ESTA\)](#) a través de la web o aplicación oficial del gobierno de EE. UU. Para ayudarles a evitar una estafa, asegúrate de hacerles saber que podrían encontrarse con sitios similares a ESTA intentando engañar a la gente para que pague de más por la solicitud. Aquí tienes otras cosas que puedes compartir con amigos o familiares que te visitan.

1. **El único lugar donde puedes solicitar es a través de la web o la app de ESTA.** Los estafadores tienen sitios web imitadores que probablemente te cobrarán de más y puede que ni siquiera entreguen tu documentación, dejándote sin los documentos de viaje que necesitas para entrar en Estados Unidos. Solicita a través de la página web oficial: [esta.cbp.dhs.gov](http://esta.cbp.dhs.gov). Los sitios similares suelen tener nombres similares, así que mira detenidamente la URL.

2. **La tasa de solicitud del ESTA no es reembolsable.** Solicitar el ESTA cuesta 10,27 \$ y no hay reembolsos, te aprueben o no. Cualquier página web que te cobre más por solicitar — o que diga que puedes obtener un reembolso — no es la web real. Ten en cuenta que, si tu solicitud es aprobada, pagarás una tasa adicional de 30 dólares... y la web oficial de ESTA solo acepta tarjetas de crédito y débito o PayPal. Si alguien te cobra más o te pide que pagues de otra manera, eso es una estafa.
3. **La información sobre el estado de la solicitud está en línea.** ¿No estás seguro de si usaste la web correcta? Confirma que ESTA tiene la información correcta y consulta el estado de tu solicitud en la [página de búsqueda de estado de la web de ESTA](#).

Para preguntas sobre su solicitud de ESTA, contacte con el Centro de Comunicaciones para Viajeros de la Oficina de Aduanas y Protección Fronteriza de EE. UU. en el 1-202-325-8000.

¿Detectar una estafa ESTA? Denúncialo a la FTC en [ReportFraud.ftc.gov](http://ReportFraud.ftc.gov).



# 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.