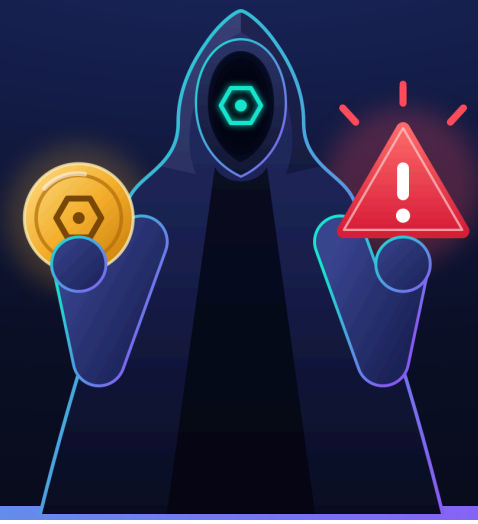
CRYPTONIMUS

Checklist antiestafas cripto

Repásala antes de enviar un solo euro. Cinco minutos de comprobación pueden ahorrarte meses de problemas.



> **Regla de oro:** si para poder cobrar o retirar tu dinero te piden que envíes más dinero (comisiones, impuestos, "desbloqueos"), **para**. Es la señal más repetida de las estafas.

1 Señales de alarma en la oferta

Marca las que se den. Si marcas **una sola**, detente y pasa a la sección 2.

- [ ] **Promete ganancias altas, rápidas o "sin riesgo".**
  Ninguna inversión en criptoactivos es segura. Quien lo asegura, miente.
- [ ] **Te presiona para decidir ya.**
  "Última oportunidad", cuentas atrás, plazas limitadas, "mañana ya será tarde".
- [ ] **Te contactó alguien que no conocías.**
  WhatsApp, Telegram, redes o un "número equivocado" que acaba en conversación amistosa o romántica.
- [ ] **Un "gurú", asesor o "amigo" te guía y te pide discreción.**
  Nadie serio te pide que no se lo cuentes a tu banco o a tu familia.
- [ ] **Te piden las palabras de recuperación (seed), claves privadas o contraseñas.**
  Ninguna empresa legítima las necesita jamás. Quien las tiene, controla tu dinero.
- [ ] **Te hacen instalar una app que no está en las tiendas oficiales o dar acceso remoto a tu equipo.**
  Es un método habitual para vaciar cuentas y wallets.
- [ ] **Te enseñan "ganancias" en una pantalla que solo ves tú para que metas más dinero.**
  Un saldo en una web o app no es dinero real hasta que puedes retirarlo.

info@cryptonimus.com

2 Comprueba quién está detrás

Marca lo que hayas verificado tú mismo. Si no puedes marcarlo, no sigas.

- [ ] **No aparece en las advertencias de la CNMV.**
  En cnmv.es, apartado «Advertencias», hay un buscador de entidades advertidas. Hay que escribir el nombre completo de la entidad.
- [ ] **Si presta servicios con criptoactivos, está en el registro de ESMA.**
  Busca la entidad en el registro provisional MiCA (proveedores autorizados) y comprueba también que no figure en la lista de entidades incumplidoras.
- [ ] **Sabes exactamente qué empresa concreta es, con domicilio y número de registro.**
  Un nombre comercial no basta. Las protecciones solo afectan a la entidad concreta que figura como autorizada.
- [ ] **No es una empresa clonada.**
  Los estafadores copian el nombre, la web o los datos de entidades legítimas. Compara dirección web, registro y datos de contacto con los oficiales.
- [ ] **Has leído reseñas independientes y recientes.**
  Busca "nombre + estafa" y "nombre + retiros". Desconfía si todas las opiniones son perfectas.
- [ ] **Te permiten retirar sin pagar nada antes.**
  Si piden comisiones, impuestos o "verificaciones" en dinero para dejarte retirar, es una estafa.

Ojo: estar en un registro significa que la entidad está autorizada, no que su producto sea bueno ni que no haya riesgo. Los criptoactivos pueden perder todo su valor.

3 Protege tu seguridad básica

Marca lo que ya tengas hecho.

- [ ] **Guardas tu frase de recuperación (seed) fuera de internet.**
  En papel o metal, en un lugar seguro. Nunca en una foto, en la nube, en notas del móvil ni en un mensaje.
- [ ] **Tienes activada la verificación en dos pasos con app.**
  Mejor una app de autenticación o una llave física que el SMS.
- [ ] **Entras a tus plataformas escribiendo la dirección tú mismo o desde un marcador.**
  No desde anuncios, mensajes ni enlaces que te llegan por sorpresa.
- [ ] **Revisas qué firmas y permisos autorizas en tu wallet.**
  Si no entiendes lo que estás firmando, no lo firmes.
- [ ] **Compras tu wallet física solo al fabricante o a distribuidores oficiales.**
  Un dispositivo "ya configurado" o de segunda mano es una trampa típica.

Contenido educativo. No constituye asesoramiento financiero ni una recomendación de inversión. Invertir en criptoactivos conlleva riesgo de perder todo el dinero invertido.

4 Si ya has caído: qué hacer

Puede pasarle a cualquiera. Lo importante es actuar con calma y rapidez.

- [ ] **Deja de enviar dinero.**
  Aunque te prometan que con un pago más recuperarás todo, no lo hagas.
- [ ] **Guarda todas las pruebas.**
  Capturas, chats, correos, direcciones de wallets, hashes de transacciones, webs y nombres usados. No borres nada.
- [ ] **Avisa cuanto antes a tu banco o a la plataforma desde la que enviaste el dinero.**
  En algunos casos pueden bloquear o investigar la operación si se actúa a tiempo.
- [ ] **Denuncia.**
  Ante la Policía Nacional o la Guardia Civil, con las pruebas ordenadas. Cuanto antes, mejor.
- [ ] **Cambia tus contraseñas y revoca permisos.**
  Si diste acceso a tu wallet, cuentas o equipo, mueve tus fondos a una wallet nueva y revisa los dispositivos.
- [ ] **Desconfía de quien te ofrece "recuperar" tu dinero.**
  Es otra estafa muy habitual: contactan con víctimas y piden un pago por adelantado. Nadie puede garantizarte recuperar lo perdido.

Resumen en una frase: si no entiendes cómo gana dinero, no puedes comprobar quién es, o te piden dinero para poder retirarlo, **no inviertas**.

Dónde comprobar y consultar

- **CNMV, Advertencias:** cnmv.es → Advertencias (buscador de entidades advertidas y entidades no autorizadas).
- **CNMV, Guía «Estafas y fraudes»:** publicación gratuita del regulador con los tipos de fraude más comunes.
- **ESMA, Registro provisional MiCA:** esma.europa.eu → MiCA (proveedores autorizados y entidades incumplidoras).

¿Quieres más? En **cryptonimus.com** encontrarás guías, alertas y casos reales analizados con datos. ¿Dudas o una estafa que quieras comentar? Escríbenos a **info@cryptonimus.com**.

Contenido educativo. No constituye asesoramiento financiero ni una recomendación de inversión. Cryptonimus no tiene licencia de asesor financiero. Versión 1.0 · Noviembre 2026.