

Documento de advertencias sobre riesgos asociados a los criptoactivos

El presente documento tiene por objeto ofrecer una advertencia clara, completa y equilibrada sobre los riesgos inherentes a los criptoactivos y a los servicios relacionados con los mismos, de conformidad con las directrices y comunicaciones emitidas por las Autoridades Europeas de Supervisión (ESMA, EBA y EIOPA por sus siglas en inglés) en marzo de 2025.

Cecabank, S.A. ("**Banco**") es una entidad de crédito autorizada para prestar determinados servicios sobre criptoactivos conforme al Reglamento (UE) 2023/1114 ("**MiCA**"), y en este ámbito actúa bajo la supervisión de la Comisión Nacional del Mercado de Valores ("**CNMV**").

El Banco no presta servicios a clientes minoristas. Sus servicios están dirigidos exclusivamente a clientes institucionales y contrapartes elegibles, quienes actúan por cuenta propia o por cuenta de sus propios clientes finales. En coherencia con su perfil profesional y la normativa MiCA, los clientes institucionales que intermedian o prestan servicios a terceros son responsables de transmitir a sus propios clientes las advertencias y riesgos inherentes a los criptoactivos y cumplir con toda la normativa aplicable en cada momento.

Esta responsabilidad incluye:

- Informar de forma veraz, clara y no engañosa sobre la naturaleza de los criptoactivos y los riesgos asociados.
- Garantizar que los clientes finales comprendan la ausencia de garantías o derechos equiparables a los productos financieros tradicionales.
- Asegurar que las comunicaciones comerciales, materiales de marketing o documentación contractual cumplan con los requisitos del Reglamento MiCA y con la normativa nacional de protección de los inversores.

Si bien, Cecabank no tiene ninguna obligación frente a los inversores finales.

Por tanto, este documento se publica de acuerdo con las exigencias de información establecidas por MiCA, no constituye material promocional ni recomendación de inversión, sino un instrumento de divulgación, en línea con el objetivo de contribuir a la educación financiera, la transparencia del mercado y la comprensión de los riesgos que la tecnología de registro distribuido (DLT) puede implicar.

Los criptoactivos representan una innovación tecnológica de gran potencial, pero también un conjunto significativo de riesgos financieros, operativos y legales que deben ser comprendidos y gestionados adecuadamente. A continuación, se incluye el listado de riesgos que en este ámbito deben considerarse.

1. Limitación del ámbito de protección

Aun cuando el Reglamento MiCA introduce por primera vez un marco normativo europeo para determinados criptoactivos y servicios, las protecciones previstas en dicho reglamento no equivalen a las aplicables a los instrumentos financieros tradicionales.

- No existe fondo de garantía de inversiones ni de depósitos que cubra pérdidas derivadas de la tenencia de criptoactivos.

- La protección de los inversores depende del tipo de criptoactivo y del proveedor, y puede ser limitada o inexistente en ciertos supuestos.
- Los derechos de los titulares (por ejemplo, de información, restitución o reclamación) varían en función del servicio y del criptoactivo.

Durante el período transitorio hasta julio de 2026, algunas entidades pueden seguir operando bajo regímenes nacionales, sin estar todavía autorizadas conforme a MiCA. En tales casos, los usuarios **no se benefician plenamente de las protecciones previstas por el Reglamento**.

2. Volatilidad y fluctuaciones extremas de precios

El valor de la mayoría de los criptoactivos —incluso aquellos regulados bajo MiCA— puede variar significativamente en cortos periodos de tiempo. Es posible incurrir en pérdidas sustanciales o totales del capital invertido.

3. Riesgos de liquidez

Los mercados secundarios de criptoactivos pueden carecer de suficiente profundidad o actividad, lo que dificulta la venta o conversión rápida de un activo al precio deseado.

4. Riesgos operativos y tecnológicos

El uso de tecnología de registro distribuido conlleva riesgos operativos específicos:

- Fallos en contratos inteligentes, errores de código o vulnerabilidades en nodos y redes.
- Pérdida o sustracción de claves privadas, que implica la pérdida irreversible del acceso a los activos.
- Dependencia de terceros subcustodios o proveedores tecnológicos, cuya solvencia o seguridad puede no estar garantizada.

5. Fraudes, ciberataques y suplantaciones

Los entornos digitales son especialmente sensibles a ataques informáticos (phishing, malware, ingeniería social). Los defraudadores pueden suplantar identidades de proveedores legítimos o utilizar nombres similares para inducir a error.

6. Información incompleta o engañosa

Algunos proyectos o criptoactivos pueden promocionarse mediante información confusa o no verificada, especialmente a través de redes sociales o canales no supervisados.

7. Complejidad y asimetría informativa

La comprensión de los factores que determinan el valor o funcionamiento de un criptoactivo requiere conocimientos técnicos y financieros avanzados. Incluso los operadores profesionales deben mantener una vigilancia constante sobre la evolución tecnológica y regulatoria.

8. Diferenciación entre criptoactivos regulados y no regulados

El Reglamento MiCA distingue entre:

- **Criptoactivos regulados:** incluyen tokens referenciados a activos (ART), tokens de dinero electrónico (EMT) y otros criptoactivos ofrecidos al público o admitidos a negociación por proveedores autorizados.
- **Criptoactivos no regulados o emitidos fuera de la UE:** no están cubiertos por MiCA y no ofrecen las garantías legales de información, gobernanza ni custodia previstas en la normativa europea.

Los clientes institucionales deben asegurarse de que todas las contrapartes y subproveedores con los que colaboren estén debidamente autorizados conforme al registro de ESMA, y deben abstenerse de realizar operaciones con proveedores no registrados o radicados fuera del Espacio Económico Europeo.