

Cripto Seguridad

Los activos virtuales son seguros y cuentan mecanismos de seguridad adecuados para evitar a ciberdelincuentes. Sin embargo, para tener mayor certeza y tranquilidad, es recomendable comprar los USDT (Tether) de empresas legalmente constituidas, reguladas y de buena reputación.

La empresa que custodia tus USDT (Tether) (activos virtuales en general) tiene que contar con sistemas de seguridad digital altamente especializados, similares a los de la Banca Digital, que cuenta con multifactores de autenticación, *tokens*, certificados digitales, entre otros.

Más aún, los USDT (Tether) están encriptados por claves criptográficas que no debes compartir con ninguna persona a través de mensajes, sms, whatsapp, llamadas o correos electrónicos, de esta manera nadie podrá tener acceso a tu cuenta digital de USDT.

Al momento de comprar, custodiar o vender activos virtuales o *Stablecoins* es mejor hacerlo a través de una empresa legalmente constituida, regulada y que cuente con la experiencia para realizar gestiones financieras locales e internacionales. Lamentablemente, muchas personas fueron estafadas por comprar o intentar hacer *trading* con personas que no conocían y que, en su mayoría, radicaban fuera del país.

Como cualquier activo (digital o real), una vez que se compra, tiene que ser resguardado y protegido. Existen dos formas para custodiar activos virtuales: físicos o digitales. Los llamados “monederos físicos” no están conectados al Internet y almacenan los activos virtuales en dispositivos personales, como discos duros o memorias USB. En cambio, los “monederos digitales” se conectan al Internet y usan mucha infraestructura tecnológica y toman medidas de ciberseguridad para proteger y resguardar los activos digitales. En ambos casos, para acceder se requieren multifactores de autenticación que no debes compartir con nadie.

La seguridad de los activos virtuales es un aspecto de responsabilidad compartida entre la empresa que custodia los USDT (Tether) y el cliente que cuida sus accesos y contraseñas.

Consejos de Seguridad

Sospecha de los mensajes desconocidos

Se debe tener mucho cuidado con los mensajes no esperados, por email, teléfono, whatsapp o redes sociales. Nunca compartas la contraseña de tu wallet o cuenta digital.

Verifica la identidad de quien te contacta

Confirma cualquier comunicación que recibas respecto a las transferencias o pagos que realices con tus USDT (Tether), contacta al sitio oficial para realizar toda consulta.

Evita Links o QR's sospechosos

Verifica todo enlace o QR que recibas por mails o mensajes. Una buena práctica es situar el puntero del ratón de la computadora sobre el enlace para comprobar la *URL* al que te direccionará. Si un enlace te ofrece descargar archivos adjuntos ¡No lo hagas! Puede ser un Spyware o Malware.

Protege tu información personal

Nunca compartas tu información personal o financiera con ninguna persona, mucho menos por enlaces que te la solicitan. Las empresas que custodian tus activos virtuales no te solicitarán información confidencial mediante email ni llamadas.

Investiga antes de realizar cualquier transacción

Antes de transferir tus USDT (Tether) o realizar pagos, verifica la compañía o persona a la que contactarás. Si es una empresa nueva para ti, consulta reseñas en busca de opiniones o experiencias de otras personas.

Protege tus dispositivos

Tienes que instalar un antivirus en la pc o dispositivo donde está la APP de *trading* o *wallet* digital, además de mantenerla actualizada. Establece contraseñas combinando letras, número y caracteres especiales y lo ideal es tener autenticación multifactor.

Para más información visita: www.bisa.com