

## PROCEDIMIENTO PARA REGISTRO DE PROVEEDORES DE SERVICIOS DIGITALES

### A. Procedimiento para registro de Proveedores de Servicios de Activos Digitales

El interesado en operar como Proveedores de Servicios de Activos Digitales, deberá solicitar su registro a la Comisión Nacional de Activos Digitales (CNAD), de conformidad con lo establecido en los artículos 9 literal d), 18, 20, 21 de la Ley de Emisión de Activos Digitales, y 7, 17 al 35 del Reglamento de Proveedores de Servicios de Activos Digitales. Para tales efectos el interesado debe completar dos etapas: la primera etapa denominada "pre inscripción" y la segunda etapa denominada "registro definitivo".

El interesado deberá seguir los siguientes pasos:

#### Completar el formulario de registro definitivo de Proveedores de Servicios de Activos Digitales

En dicho formulario deberá completarse con la siguiente información:

- 1) **Plan de Negocios** a desarrollar en El Salvador para los próximos 3 años:
  - Resumen Ejecutivo
  - Descripción del Negocio
  - Estrategia de Mercado
  - Proyecciones Financieras
  - Presupuesto de Gastos
  - Indicadores Clave de Rendimiento (KPIs)
  - Riesgos y Mitigaciones
  - Implementación y Seguimiento
  - Resumen y Conclusiones
- 2) Documentación acerca de la aplicación de "**Sistema de atención a los usuarios/Comunicación con el Cliente**", según el artículo 7 literal f) y artículo 22 del Reglamento de Proveedores de Servicios de Activos Digitales, el cual deberá contener los requerimientos mínimos:
  - Una explicación general de cada activo digital que debe incluir sus características más relevantes, tales como su intercambiabilidad con otros activos digitales, su precio actual, su historial de precios durante los últimos doce meses y el volumen de operación que

tiene actualmente en la plataforma o billetera digital. La actualización de esta información debe ser regular y razonable de acuerdo al producto.

- La forma en que se pueden vender y comprar activos digitales en la plataforma o billetera digital que administre o promueva el proveedor de servicios de activos digitales.
- Comisiones aplicables a la transacción.
- Lista y explicación del resto de productos complementarios que ofrece, tales como custodia, préstamos y formas de depósitos. La actualización de esta información debe ser regular y razonable de acuerdo con el producto.
- Política de atención que incluya los canales y protocolos de su sistema de atención a los usuarios de forma coherente y eficiente de acuerdo a la naturaleza de los servicios que prestará.

**NOTA:** En todo momento, los Proveedores de Servicios de Activos Digitales deberán tener toda la información relevante respecto a los servicios y a los activos digitales que comercializan o administran disponible en su dirección de LRU. La actualización de esta información debe ser regular y razonable de acuerdo con el producto.

3) Documentación acerca de la aplicación de **“Prevención de Lavado de Activos, Financiamiento del Terrorismo y La Proliferación de Armas de Destrucción Masiva”**, según los artículos 17, 19, 23 y 24 del Reglamento de Proveedores de Servicios de Activos Digitales:

- Inscripción ante la Unidad de Investigación Financiera del Oficial de Cumplimiento Titular y Suplente;
- Nombramiento según la junta directiva de los Oficiales de Cumplimiento Titular y Suplente;
- Certificación del Oficial de Cumplimiento Titular y Suplente en materia de LA/FT/FPADM según lo establecido en el artículo 64 del instructivo de la Unidad de Investigación Financiera para la Prevención del Lavado de Dinero y de Activos;
- Organigrama que incluya la Oficialía de Cumplimiento;
- Planeación y administración con un enfoque basado en riesgos;
- Documentación, archivo y conservación de documentos;
- Política de Prevención de LA/FT/FPADM;
- Procedimientos de Gestión de Riesgo de LA/FT/FPADM;
- Política de límites de transacciones con Activos Digitales;

- Política de Debida Diligencia de Clientes (estándar e intensificada) y Personas Políticamente Expuestas;
  - Política de Monitoreo de operaciones de Clientes y Contrapartes;
  - Políticas para evitar el robo de activos
  - Código de Ética Institucional:
    - El cual deberá incluir el apartado “Buena Fe e Imparcialidad en los Mercados de Activos Digitales” según el artículo 17 del Reglamento de Proveedores de Servicios de Activos Digitales; y el apartado “Prohibiciones del Uso de Información Privilegiada” según los artículos 23 y 24 del Reglamento de Proveedores de Servicios de Activos Digitales.
  - Procedimientos de detección de Operaciones Inusuales y Sospechosas (Incluir procedimiento con flujograma de la implementación del monitoreo de operaciones inusuales y elaboración de reportes de operaciones sospechosas);
  - Procedimiento de Reporte de Operaciones Reguladas según el artículo 52, literal b) del Instructivo de la Unidad de Investigación Financiera para la Prevención del Lavado de Dinero y de Activos:
    - Reportes de operaciones requeridos por la UIF;
    - Registro de clientes para identificar origen y destino de los fondos;
    - Registro de activos, pasivos y patrimonio;
    - Registro de cuentas con datos de las transacciones;
    - Registro de quejas;
    - Plan de capacitación.
- 4) Documentación acerca de la aplicación de “**Factores de Riesgo**”, según el artículo 21 del Reglamento de Proveedores de Servicios de Activos Digitales:
- Descripción de los riesgos al que está expuesta la entidad dado su modelo de negocio (Incluir riesgos financieros y operacionales, no solamente LA/FT/FPADM y ciberseguridad).
  - Responsabilidades a las áreas de gobierno corporativo en el marco de gestión integral de riesgos
  - Descripción de las actividades o herramientas que constituyen cada etapa del ciclo de gestión de los riesgos (Identificación, medición, monitoreo, mitigación y comunicación del riesgo)



COMISIÓN NACIONAL DE  
ACTIVOS DIGITALES

- Las medidas que se adoptarán para prevenir posibles incumplimientos a requerimientos regulatorios y las que adoptarán en el evento de que haya incurrido en ellos, debiendo definir en ambas situaciones los parámetros que orientarán la actuación y los responsables de implementarlas.
- 5) Documentación acerca de la aplicación de “**Operaciones en Activos Digitales**”, según los artículos del 27 al 35 del Reglamento de Proveedores de Servicios de Activos Digitales:
- Operaciones al contado (artículo 28 del Reglamento)
  - Operaciones a plazo (artículo 29 del Reglamento)
  - Operaciones opcionales de compra o de venta (artículo 30 del Reglamento)
  - Liquidación de operaciones (artículo 31 del Reglamento)
  - Embargo (artículo 32 del Reglamento)
  - Arbitraje (artículo 33 del Reglamento)
  - Protección de activos de los adquirentes (artículo 34 del Reglamento)
  - Inversiones (artículo 35 del Reglamento)
- 6) Políticas y Procedimientos de Seguridad y Custodia:
- Política de Custodia de Activos Digitales y FIAT: Descripción detallada de las políticas y procedimientos para la custodia segura de activos digitales y monedas fiduciarias.
  - Políticas de Seguridad de la Información y Ciberseguridad: Este documento consolidado establece las políticas y procedimientos integrales para proteger los activos de información y tecnológicos, abarcando control de accesos, gestión de vulnerabilidades, respuesta a incidentes y formación en seguridad. Su objetivo es asegurar la confidencialidad, integridad y disponibilidad de la información, alineándose con las normativas de protección de datos.
- 7) Marco Integral de Cumplimiento y Conocimiento del Cliente/Empresa:
- Protocolo KYC (Know Your Customer) y KYB (Know Your Business): Descripción de los procedimientos de identificación y verificación de clientes/empresas para prevenir el fraude y el lavado de dinero.
  - Protocolo KYT (Know Your Transaction): Sistemas y procesos para el monitoreo y análisis de transacciones en busca de actividades sospechosas.
- 8) Gestión de Riesgos y Planificación de la Continuidad:



COMISIÓN NACIONAL DE  
ACTIVOS DIGITALES

- Políticas de Gestión de Riesgos: Establece el marco y los procesos para identificar, evaluar, gestionar y monitorear los riesgos operativos, financieros y tecnológicos. Proporciona una metodología para la toma de decisiones basada en el riesgo y para la mitigación de riesgos a niveles aceptables.
  - Plan de Continuidad del Negocio: Describe los procedimientos y medidas que deben tomarse para asegurar la continuidad operativa en caso de una interrupción significativa. Incluye la identificación de funciones críticas, la asignación de recursos para la recuperación y estrategias para mantener las operaciones durante y después de un incidente.
  - Plan de contingencia: Proporciona un enfoque estructurado para responder a incidentes imprevistos que puedan afectar gravemente las operaciones. Se centra en la restauración rápida de los servicios críticos, minimizando el impacto en el negocio y sus clientes.
- 9) Auditorías y Tecnologías de Control:
- Auditorías Internas/Externas: Información sobre los procesos de auditoría interna y externa, incluyendo frecuencia, alcance, y entidades auditoras.
  - Implementación de Geofencing: Detalles sobre las tecnologías y políticas de geofencing utilizadas para restringir transacciones en jurisdicciones específicas.

Luego de completar el formulario y enviarlo, deberá presentar una copia del mismo firmado por la persona autorizada para tramitarlo, junto con su documentación anexa, en formato físico en las oficinas de la Comisión. Una vez recibido, el departamento de Registro emitirá una constancia de recepción del formulario, de conformidad con el artículo 8 inciso primero y segundo del Reglamento de Proveedores de Servicios de Activos Digitales (RPSAD).