



GLOBAL FINANCIAL INTEGRITY



CYRUS R. VANCE CENTER
FOR INTERNATIONAL JUSTICE

EL ECOSISTEMA DE ACTIVOS VIRTUALES EN EL SALVADOR: Riesgos y desafíos para contrarrestar delitos financieros



Diciembre de 2024

DICIEMBRE DE 2024

EL ECOSISTEMA DE ACTIVOS VIRTUALES EN EL SALVADOR: RIESGOS Y DESAFÍOS PARA CONTRARRESTAR DELITOS FINANCIEROS

Por Global Financial Integrity
y el Cyrus R. Vance Center for International Justice

Derechos Reservados/Copyright ©2023 por Global Financial Integrity®. Algunos derechos son reservados. El reporte se ha publicado conforme a una licencia Creative Commons Attribution License (CC BY). Para más información sobre esta licencia, visite: <https://creativecommons.org/>

Portada y diseño realizado por Maria Isabel Gaviria.

AGRADECIMIENTOS

La investigación, redacción y elaboración de este informe estuvo a cargo de Global Financial Integrity (GFI) y el Cyrus R. Vance Center for International Justice.

GLOBAL FINANCIAL INTEGRITY (GFI)

GFI es un centro de pensamiento con sede en Washington, DC, que se enfoca en los flujos financieros ilícitos, la corrupción, el comercio ilícito y el lavado de dinero y activos. A través de análisis de alto impacto, de apoyo con argumentos basados en hechos para promover la propiedad de los beneficiarios finales y de una base de datos en nube para reducir el fraude comercial. GFI se ha propuesto abordar los daños infligidos por la facturación comercial indebida, la delincuencia transnacional, la evasión fiscal y la cleptocracia. GFI busca crear un mundo más seguro y equitativo trabajando con socios para aumentar la transparencia en el sistema financiero global y así promover la integridad comercial.

CYRUS R. VANCE CENTER FOR INTERNATIONAL JUSTICE

The Cyrus R. Vance Center for International Justice del Colegio de Abogados de la Ciudad de Nueva York promueve la justicia global mediante la participación de abogados de todo el mundo en apoyo de la sociedad civil y de una profesión jurídica éticamente activa. El Centro Vance es una alianza única de abogados internacionales que cataliza la innovación de interés público y reúne a los principales despachos de abogados y otros socios de todo el mundo para ser pioneros en iniciativas de justicia internacional y proporcionar representación legal sin fines de lucro a las ONG de justicia social. A través de su Programa de Buena Gobernanza y otras iniciativas programáticas, el Centro Vance persigue la transparencia y la honestidad en el gobierno, apoyando una sociedad civil robusta, la integridad judicial y el periodismo independiente, con el fin de responsabilizar a funcionarios e instituciones.

El Centro Vance agradece a los despachos de abogados pro-bono que participan en la investigación de legislaciones, normativas y mejores prácticas.

DISCLAIMER

Este informe analiza los riesgos de delitos financieros, identifica indicadores de alerta e incluye actualizaciones de la legislación pertinente en El Salvador hasta octubre de 2024. Cabe señalar que la evaluación de riesgos y la identificación de indicadores de alerta no significan que haya ocurrido un delito. Hay muchas razones legítimas por las que el comportamiento financiero puede parecer inusual; una anomalía no indica actividad ilícita. La mención de casos, empresas o países concretos en este informe no debe interpretarse como una acusación de delito; se incluyen únicamente con fines educativos.

Las conclusiones y análisis de este informe no representan necesariamente las opiniones de ninguno de los autores, evaluadores u organizaciones participantes.

CONTENIDO

Lista de acrónimos y términos	6
Resumen ejecutivo	8
Conceptos clave y definiciones	12
Introducción y contexto de El Salvador	18
Capítulo 1. Marco legal para la prevención del lavado de dinero y activos en El Salvador	32
A. Marco Normativo	33
Ley Contra el Lavado de Dinero y Activos (LCLDA) vigente (1998)	34
Anteproyecto Ley Especial Para la Prevención, Control y Sanción del Lavado de Activos, Financiamiento al Terrorismo y de la Proliferación de Armas de Destrucción Masiva de 2023 (APL)	35
Ley de Emisión de Activos Digitales y sus reformas	37
B. Marco Institucional	39
Unidad de Investigación Financiera (UIF)	39
Reportes de Operaciones Sospechosas (ROS)	39
Debida diligencia del Cliente (DDC)	40
Personas Políticamente Expuestas (PEP)	41
Beneficiarios Finales	42
Sujetos Obligados (SO)	43
Proveedores de Servicios de Activos Virtuales (PSAV)	44
(i) Aplicación de estándares ALA/CFT	44
(ii) Evaluación de Riesgo (ER) y Enfoque en Políticas Aplicables a los PSAV	48
Obligaciones de Reporte de Operaciones Sospechosas para PSB y PSAD	49
Beneficiarios Finales (BF) y PSB/PSAD	51
La Regla del Viajero	51
Debida Diligencia del Cliente y PSAV	52
Cooperación internacional: Investigación de cuentas de PSAD, congelación/incautación y recuperación de activos	53

Capítulo 2: Riesgos del Ecosistema de AV y Delitos Financieros	54
AV y Riesgos de Delitos Financieros en El Salvador	54
Ciudadanía por Inversión (CBI)	57
Tokenización de Activos del Mundo Real	57
Tokenización de productos agrícolas	58
Tokenización de deudas y fondos	60
La emisión de Stablecoins	62
Financiamiento Político (FP)	63
 Capítulo 3: PSAV en El Salvador y la Protección de Datos Marco Legal de Protección de Datos en El Salvador	67
A. Referencia internacional	67
(i) Reglamento General de Protección de Datos (RGPD)	67
(ii) Ley Gramm-Leach-Bliley (LGLB)	69
B. Chivo Wallet: Política de Privacidad, Términos y Condiciones	70
C. Billeteras de Activos Virtuales	72
D. Análisis comparativo de billeteras de AV	73
 Recomendaciones	75
Recomendaciones para contrarrestar delitos financieros	75
Recomendaciones para prevenir el LA/FT/PADM	76
Recomendaciones sobre financiamiento político	76
Recomendaciones sobre tokenización de activos del mundo real	77
Recomendaciones sobre protección de datos personales	78

LISTA DE ACRÓNIMOS Y TÉRMINOS

ACRÓNIMOS	EXPLICACIÓN
AAB	Agencia Administradora de Fondos Bitcoin
AD	Activos Digitales
ALA	Anti-Lavado de Activos
APL	Anteproyecto Ley Especial Para la Prevención, Control y Sanción del Lavado de Activos, Financiamiento al Terrorismo y de la Proliferación de Armas de Destrucción Masiva de 2023
APNFD	Actividades y Profesiones no Financieras Designadas
AV	Activos Virtuales
BCR	Banco Central de Reserva
BF	Beneficiario Final
BTC	Bitcoin
CBI	Ciudadanía por inversión
DDC	Debida Diligencia del Cliente
CFTC	Commodity Futures Trading Commission
CIPLAFT	Comité Interinstitucional para la prevención, control y represión del lavado de activos y el financiamiento del terrorismo y de la proliferación de armas de destrucción masiva
CMV	Comisión del Mercado de Valores
CNAD	Comisión Nacional de Activos Digitales
CFT	Contra el Financiamiento del Terrorismo
DeFi	Finanzas descentralizadas
DIR	Documento de Información Relevante
EM	Evaluación Mutua
ETH	Ether
GAFI	Grupo de Acción Financiera Internacional
GAFILAT	Grupo de Acción Financiera de Latinoamérica
GOES	Gobierno de El Salvador
FT	Financiamiento del terrorismo

KYC	Conoce a tu cliente (Know Your Customer)
LA	Lavado de activos
LB	Ley Bitcoin
LCLDA	Ley Contra el Lavado de Dinero y Activos
LEAD	Ley de Emisión de Activos Digitales
LECDIC	Ley Especial contra Delitos Informáticos y Conexos
MASI	Material de Abuso Sexual Infantil
OFAC	Oficina para el Control de Activos Extranjeros
ONBTC	Oficina Nacional del Bitcoin
PADM	Proliferación de Armas de Destrucción Masiva
PEP	Personas Políticamente Expuestas
PSAD	Proveedores de Servicios de Activos Digitales
PSB	Proveedor de Servicios Bitcoin
PSAV	Proveedores de Servicios de Activos Virtuales
SSF	Superintendencia del Sistema Financiero
TRD	Tecnología de Registro Distribuido
TIC	Tecnologías de la información y la Comunicación
UIF	Unidad de Investigación Financiera
USDT	Tether
KYB	Know Your Business
KYT	Know Your Transactions

RESUMEN EJECUTIVO

El presente informe examina en detalle la evolución del ecosistema de activos virtuales de El Salvador, ofreciendo una perspectiva amplia sobre la innovación tecnológica, la prevención de los delitos financieros y de la protección de datos, en relación con la responsabilidad de las entidades gubernamentales. La adopción de Bitcoin como moneda de curso legal en el país ha creado un entorno único y dinámico, presentando tanto oportunidades notables como desafíos. Este informe busca proporcionar una evaluación técnica del panorama actual, destacando los avances logrados.

I. EL MARCO LEGAL EN EL SALVADOR SOBRE ANTI-LAVADO DE DINERO Y CONTRA EL FINANCIAMIENTO DEL TERRORISMO

El marco legal de El Salvador para la prevención del lavado de dinero y la financiación del terrorismo (LD/FT) demuestra un compromiso con la alineación a los estándares internacionales como el Grupo de Acción Financiera Internacional (GAFI) y el Grupo de Acción Financiera de Latinoamérica (GAFILAT). Adicionalmente los esfuerzos legislativos recientes, incluidas las enmiendas propuestas como el Proyecto de Ley para la Prevención del Lavado de Dinero, la Financiación del Terrorismo y la Proliferación de Armas de Destrucción Masiva, representan un paso hacia el fortalecimiento del entorno regulatorio, permanecen importantes oportunidades de fortalecimiento.

La reciente estructura regulatoria, a través de las reformas a la Ley de Emisión de Activos Digitales, otorgan a la Comisión Nacional de Activos Digi-

tales (CNAD) plenos poderes como regulador, supervisor y sancionador, incluyendo la supervisión de los Proveedores de Servicios de Bitcoin (PSB) y los Proveedores de Servicios de Activos Digitales (PSAD). Por otro lado, la reforma incorpora a Bitcoin como parte del ecosistema de activos digitales. Adicionalmente, la CNAD sería responsable de supervisar cualquier actividad relacionada con Bitcoin, así como también de autorizar la emisión de activos digitales y monedas estables, al igual que cada uno de los actores participantes dentro de estas emisiones.

De parte del sector público, es importante promover una aplicación clara y consistente, junto con recursos suficientes dedicados a la supervisión e investigación. Ello, para promover una cooperación internacional y la coordinación interinstitucional efectiva. Adicionalmente, la colaboración entre el sector privado y público también representa una oportunidad para prevenir delitos financieros.

II. AMENAZAS EMERGENTES EN EL ECOSISTEMA DE ACTIVOS VIRTUALES EN EL SALVADOR

El ecosistema de activos virtuales en El Salvador revela potenciales riesgos que podrían ser explotados para actividades ilícitas. Algunos riesgos mencionados en el reporte examinan diversos incidentes de fraude, estafas y lavado de dinero relacionados con criptomonedas destacando las vulnerabilidades en la adopción de nuevas tecnologías.

Es importante resaltar que es necesario contar con una infraestructura sólida de seguridad de la información y de protocolos de protección de datos, para mantener la transparencia y supervisión regula-

toria; y así evitar que los consumidores sean vulnerables a delitos de suplantación de identidad, robo, entre otros.

Adicionalmente, las tecnologías emergentes que incluyen la adopción de finanzas descentralizadas y la emisión de tokens a través de contratos inteligentes, representan un elemento clave para promover la inversión. Sin embargo, los ciberdelincuentes también han utilizado esta infraestructura para explotarla, lo que hace que los estándares de seguridad de la información sean necesarios para prevenir su mal uso o explotar su potencial vulnerabilidad.

III. PROTECCIÓN DE DATOS

A la fecha de cierre de este informe, no ha sido aprobada en El Salvador una ley específica que proteja y regule la materia en un contexto de avances tecnológicos, que cuente con supervisión regulatoria y mitigue riesgos de privacidad de usuarios y seguridad financiera. La existente Ley de Acceso a la Información Pública (LAIP) proporciona cierta protección de datos, pero no aborda un marco integral requerido para el ecosistema digital en evolución.

IV. RECOMENDACIONES

Este informe concluye con una serie de recomendaciones específicas que pueden apoyar la capacidad de El Salvador de prevenir y mitigar eficazmente los delitos financieros. Entre las principales recomendaciones figuran las siguientes:

Fortalecer el Marco Regulatorio de ALA/CFT en El Salvador: Priorizar evaluaciones de riesgo integrales, fortalecer la supervisión de PSAV y agilizar los mecanismos de intercambio de información con socios internacionales.

Promulgar una Ley de Protección de Datos: Implementar una ley de protección de datos que incorpore buenas prácticas internacionales, asegurando la privacidad del usuario, medidas de seguridad robustas y una implementación efectiva.

Robustecer la Infraestructura de Seguridad de la Información: Invertir en modernizar la infraestructura nacional de ciberseguridad y evitar el uso de la tecnología para fines ilícitos.

Fortalecer la Transparencia y Supervisión de la Financiación Política: Introducir regulaciones sólidas y transparentes que rijan la financiación de partidos políticos y campañas, con disposiciones explícitas para la declaración y verificación de donaciones y transferencias realizadas utilizando activos virtuales.

Promover la Colaboración y Educación: Fomentar la colaboración entre los actores principales del sector público y privado, mejorando el intercambio de información y los esfuerzos ALA/CFT.

Invertir en Campañas de Concienciación Pública: Promover la alfabetización financiera y las mejores prácticas de ciberseguridad a través de campañas de concienciación pública generalizadas.

El camino de El Salvador para integrar Bitcoin en su economía presenta un estudio de caso sobre los desafíos y oportunidades inherentes en la navegación del mundo en rápida evolución de los activos virtuales. El país ha demostrado una disposición para fomentar la innovación a través de la adopción de Bitcoin y a través de la promoción de la emisión de activos digitales como monedas estables y tokens que representan deudas, fondos o productos agrícolas; los hallazgos presentados en este informe resaltan una oportunidad de una adecuada implementación del marco regulatorio para mitigar los riesgos de delitos financieros y proteger la privacidad de sus ciudadanos.

CONCEPTOS CLAVE Y DEFINICIONES

Activos Digitales (AD): Representación digital que se puede almacenar o transferir electrónicamente utilizando tecnologías como Blockchain, DLT u otros similares, donde los registros están vinculados y protegidos por métodos de encriptación para asegurar la privacidad de las transacciones. Los activos digitales pueden ser adquiridos por individuos o empresas para intercambiarlos, transferirlos, negociarlos o promoverlos.¹

Activos Virtuales (AV): “Cualquier representación digital de valor que se pueda comercializar, transferir o usar para pagos de forma digital”. Esto no incluye tokens no fungibles (NFT) como coleccionables ni representaciones digitales de monedas fiduciarias.²

Beneficiario Final (BF): Según el Grupo de Acción Financiera Internacional, se refiere a la persona física que “en última instancia posee o controla a un cliente y/o la persona física en cuyo nombre se realiza una transacción.”³

Bitcoin (BTC): La primera criptomoneda y moneda virtual descentralizada. Los bitcoins son unidades de cuenta compuestas por cadenas únicas de números y letras que constituyen unidades de la moneda y tienen valor sólo porque las personas están dispuestas a pagar por ellos. Bitcoin funciona con tecnología blockchain, que está compuesta por dos partes: nodos y mineros.⁴

Certificador: Persona jurídica encargada de realizar un análisis financiero, legal, técnico y administrativo del material y la información relevante de las ofertas públicas contenidas en el Documento de Información Relevante (DIR). Una vez realizado el análisis, el certificador emite y presenta un informe sobre el cumplimiento del emisor con las obligaciones formales y sustantivas ante la Comisión Nacional de Activos Digitales.⁵

Conozca a su Cliente (KYC): Conjunto de procedimientos que permiten a los bancos y otras entidades financieras confirmar la identidad de las organizaciones y personas con los que realizan operaciones financieras para asegurarse de que actúan dentro del marco legal.⁶

¹ Asamblea Legislativa de El Salvador. (2023). Ley de Emisión de Activos Digitales. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/OCDA225C-1B6C-4098-AC3A-D608933C643B.pdf>

² Financial Action Task Force. (2014). Virtual currencies: Key definitions and potential AML/CFT risks. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

³ Financial Action Task Force. (2014). FATF Guidance. Transparency and Beneficial Ownership. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-transparency-beneficial-ownership.pdf>

⁴ Financial Action Task Force. (2014).

⁵ Asamblea Legislativa de El Salvador. (2023). Ley de Emisión de Activos Digitales. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/OCDA225C-1B6C-4098-AC3A-D608933C643B.pdf>

⁶ Society of Worldwide Interbank Financial Telecommunication. (s.f.) The KYC process explained. <https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/kyc-process>.

Corrupción: Se refiere al “abuso de la función pública para beneficio privado. Abarca una amplia gama de comportamientos, desde el soborno hasta la apropiación de fondos públicos”.⁷

Criptojackning: Cibercrimen en el que un criminal aprovecha secretamente la capacidad de procesamiento virtual de una víctima para generar criptomonedas. Una de las modalidades más frecuentes ocurre cuando la víctima instala inadvertidamente un programa con scripts maliciosos que permiten al victimario acceder a la computadora u otro dispositivo conectado a internet.⁸

Debida Diligencia del Cliente (DDC): Proceso empleado por las instituciones financieras para reunir y analizar información sobre un cliente o potencial cliente.⁹

Documento de Información Relevante (DIR): “Documento que proporciona al público información esencial sobre una oferta pública de activos digitales. Incluye la identificación del emisor, las características y los objetivos de la emisión. Además, debe especificar si los intereses, ingresos, rendimientos o

beneficios de la oferta pública serán pagados con dinero escritural o en activos digitales”.¹⁰

Emisor: Persona natural o jurídica, privada o pública, que realiza una oferta pública de activos digitales para venderlo o comercializarlo en una plataforma de intercambio.¹¹

Ether (ETH): Cripto activo basado en una blockchain descentralizada que establece una red peer to peer que permite a las personas coordinarse, hacer acuerdos o transferir activos digitales entre ellos.¹²

Finanzas Descentralizadas (DeFi): Se refiere a la provisión de servicios financieros sin la necesidad de un custodio intermediario que no sea basado en blockchain.¹³

Mixer o Tumbler: Un mezclador de criptomonedas es un servicio que combina las criptomonedas de muchos usuarios para ocultar los orígenes y propietarios de los fondos. Debido a que Bitcoin, Ethereum y la mayoría de las otras blockchains públicas son transparentes, este nivel de privacidad es difícil de alcanzar de otra manera.¹⁴

⁷ World Bank. (2020). Anti Corruption Fact Sheet <https://www.world-bank.org/en/news/factsheet/2020/02/19/anticorruption-fact-sheet>.

⁸ Interpol. (s.f). What is Cryptojacking? How does it work?. <https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking>.

⁹ Society of Worldwide Interbank Financial Telecommunication. (s.f.) What is Customer Due Diligence (CDD). [https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/customer-due-diligence-cdd#:~:text=Due%20Diligence%20\(CDD\)-,What%20is%20Customer%20Due%20Diligence%20\(CDD\)%3F,a%20customer%20or%20potential%20customer](https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/customer-due-diligence-cdd#:~:text=Due%20Diligence%20(CDD)-,What%20is%20Customer%20Due%20Diligence%20(CDD)%3F,a%20customer%20or%20potential%20customer).

¹⁰ Asamblea Legislativa. (2023). Ley de Emisión de Activos Digitales. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/OCDA225C-1B6C-4098-AC3A-D608933C643B.pdf>

¹¹ Asamblea Legislativa. (2023).

¹² Ethereum. (s.f.). What is Ethereum, <https://ethereum.org/en/what-is-ethereum/>.

¹³ National Institute of Standards and Technology. understanding stablecoin technology and related security considerations. (2023). <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8408.pdf>.

¹⁴ Chainalysis Team. (2022). Crypto mixers and AML Compliance. “<https://www.chainalysis.com/blog/crypto-mixers/>

Moneda estable o stablecoin: Activo digital que tiene un valor estable y está respaldado por una o varias monedas fiduciarias u otro activo subyacente de baja volatilidad.¹⁵

Proliferación de Armas de Destrucción Masiva (PADM): Se refiere a la “fabricación, adquisición, posesión, desarrolló, exportación, transbordo, intermediación, transporte, transferencia, almacenamiento o uso de armas nucleares, químicas o biológicas y sus medios de entrega y materiales relacionados (incluyendo tanto tecnologías y bienes de doble uso utilizados para fines no legítimos)”.¹⁶

Proveedor de Servicios de Activos Digitales (PSAD): “Cualquier persona física o jurídica cuya actividad profesional implique la prestación de servicios relacionados con activos digitales. Esto incluye, entre otros, el intercambio de activos digitales por dinero fiduciario o equivalente, o por otros activos digitales, ya sea utilizando su propio capital o capital de terceros; la operación de una plataforma de intercambio o negociación de activos digitales o derivados; y la colocación de activos digitales en plataformas digitales o billeteras”.¹⁷

Proveedor de Servicios de Activos Virtuales (PSAV): “Cualquier persona física o jurídica que realice una o más de las siguientes actividades u operaciones por cuenta propia o en nombre de otra: i. Intercambio entre activos virtuales y monedas de curso legal; ii. Intercambio entre una o más formas de activos virtuales; iii. Transferencia de activos virtuales; iv. Custodia y/o administración de activos virtuales o instrumentos que permitan el control sobre activos virtuales; v. proveeduría de servicios financieros relacionados con la oferta y/o venta de un activo virtual por parte de un emisor”.¹⁸

Ransomware: Malware que impide que una persona acceda a su dispositivo y datos almacenados, generalmente mediante el cifrado de los archivos. Para recuperar dicha información, el criminal exigirá un rescate o extorsión.¹⁹

Sandbox regulatorio: Es un entorno de pruebas cerrado, diseñado para experimentar de forma segura con proyectos de desarrollo web o de software, siendo un campo de pruebas para nuevos modelos de negocio que aún no están protegidos por una regulación vigente, supervisados por las instituciones regulatorias.²⁰

¹⁵ Ministerio de Economía de El Salvador, Reformas a la Ley de Activos Digitales, 2024.

¹⁶ Financial Action Task Force.(2021). Guidance on proliferation financing risk assessment and mitigation. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf>.

¹⁷ Global Financial Integrity and Vance Center. (2023). The Virtual Assets Ecosystem In El Salvador: Strengthening Financial Integrity And Transparency. <https://34n8bd.p3cdn1.secureserver.net/wp-content/uploads/2023/10/Crypto-El-Salvador-Report-ENG-FINAL-1.pdf?time=1719550890>.

¹⁸ Financial Action Task Force. (2021). Virtual assets and virtual asset service providers. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf>.

¹⁹ National Cyber Security Center .(s.f.). A guide to ransomware, United Kingdom. <https://www.ncsc.gov.uk/ransomware/home>.

²⁰ BBVA. Comunicaciones. (2017). ¿Qué es un Sandbox Regulatorio?. <https://www.bbva.com/es/que-es-un-sandbox-regulatorio/>

Tecnología de Registro Distribuido: “Tecnología que tiene como objetivo generar un registro distribuido en un ambiente digital interconectado por una red de datos”.²¹

Token: Un activo digital que se utiliza como unidad de cuenta en una red, basado en Tecnología de Registro Distribuido o una tecnología similar o análoga.²²

Tokenización: Es el proceso de transformar la propiedad y los derechos de activos específicos en una forma digital. Mediante la tokenización, se pueden convertir activos indivisibles, en forma de token.²³

Trata de Personas: También conocida como “trata”, es un “delito que implica obligar o coaccionar a una persona a proporcionar trabajo o servicios, o a participar en actos sexuales comerciales. La coacción puede ser sutil o manifiesta, física o psicológica”.²⁴

²¹ Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, DLT/BLOCKCHAIN Borrador - Guía para el uso y la implementación de tecnología de registros distribuidos (DLT/Blockchain) en el sector público, https://mintic.gov.co/portal/715/articles-149959_recurso_1.pdf

²² Blockchain Council. (2023). What is Tokenization? A complete guide, <https://www.blockchain-council.org/blockchain/what-is-tokenization/>.

²³ Blockchain Council. (2023).

²⁴ U.S. Department of Justice. (2023). What is human trafficking?. <https://www.justice.gov/humantrafficking/what-is-human-trafficking>.

INTRODUCCIÓN Y CONTEXTO DE EL SALVADOR

El Salvador cuenta con un marco normativo nacional para asegurar la transparencia e integridad,²⁵ así como para combatir flujos financieros ilícitos relacionados con el lavado de activos (LA). Este marco normativo se alinea con las recomendaciones y principios de organismos internacionales. El país ha diseñado e implementado legislación para fomentar la innovación tecnológica y combatir delitos mediante el uso de las Tecnologías de la Información y la Comunicación (TIC). En este contexto, también ha adoptado diversas regulaciones en torno a los activos virtuales (AV). Para efectos de este informe, se utilizará el término activos digitales o activos virtuales indistintamente, ya que, bajo el marco regulatorio de El Salvador, el término utilizado es activos digitales y bajo los estándares del Grupo de Acción Financiera Internacional (GAFI), se utiliza el término activos virtuales.

Desde la perspectiva internacional, El Salvador participó en las sesiones de evaluación del Grupo de Acción Financiera de Latinoamérica (GAFI-LAT) entre el 8 y 19 de enero de 2024, cuyos resultados fueron publicados en agosto de ese mismo

año²⁶. Estos incluyen la evaluación de las medidas implementadas contra el lavado de activos (ALA) y contra el financiamiento del terrorismo (CFT), así como el nivel de cumplimiento de las 40 Recomendaciones del GAFI, incluyendo la recomendación 15 sobre la utilización de nuevas tecnologías el cual se encuentra estrictamente relacionado a los activos virtuales.

ECOSISTEMA FINANCIERO Y TECNOLÓGICO EN EL SALVADOR

El ecosistema financiero y tecnológico de El Salvador es diverso, sobre todo en lo que respecta a su regulación e incorporación de nuevas tecnologías. Además, es pertinente considerar la adopción pionera de Bitcoin como moneda de curso legal en el país, su uso, y el de otros activos virtuales por parte de la población.

La población de El Salvador no sobrepasa los 6,338,900 millones de habitantes²⁷. De esta cifra, el 88% de los salvadoreños no utilizó Bitcoin durante 2023, y un 48.8% está en desacuerdo con el gasto público destinado a su adopción²⁸. Aunque la adopción del Bitcoin como moneda de curso legal busca impulsar el desarrollo económico de El Salvador, entre 2019 y 2024, el 80.5% de salvadoreños indicó no haber recibido beneficios económicos del uso del Bitcoin, y el 66.6% cree que

²⁵ El marco normativo de transparencia en El Salvador incluye leyes que regulan acciones de funcionarios públicos y particulares. Entre estas: el Código Penal, Ley de Bancos, y normativa CLDA y la corrupción. Aunque se establecen medidas de conducta y sanciones, la falta de control ha limitado su efectividad. La corrupción privada también afecta el desarrollo económico y la democracia, por lo que es necesario un enfoque estratégico basado en la gestión del riesgo anticorrupción para fortalecer la transparencia en todos los sectores.

²⁶ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. Informe de Evaluación Mutua de la República de El Salvador – GAFILAT

²⁷ Banco Central de Reserva de El Salvador, "Población", 2023. <https://estadisticas.bcr.gob.sv/serie/poblacion?lang=es>

²⁸ La Prensa Gráfica. (2024). Bitcoin no termina de convencer a los salvadoreños. Bitcoin no termina de convencer a los salvadoreños - La Prensa Gráfica (laprensagrafica.com)

la criptomoneda no ha mejorado su situación familiar.²⁹ A pesar de ello, el gobierno sigue impulsando la adopción de tecnologías financieras y especialmente de activos digitales, con el objetivo de mejorar la inclusión digital y la prosperidad de la economía.

Por otro lado, el Gobierno de El Salvador busca un impulso digital y financiero que pueda ser aprovechado por su población, a través de una Política Nacional de Inclusión Financiera. Es importante también considerar que el 64% de la población de El Salvador continúa sin acceso a servicios bancarios,³⁰ y solo el 11% tiene cuentas a través de teléfonos móviles (eMoney).³¹ Así, la implementación de la Política Nacional de Inclusión Financiera³² representa oportunidades para incorporar la digitalización e innovación financiera, y establece a la transformación digital como una prioridad en su Agenda Digital 2020-2030.³³³⁴

Adicionalmente para promover el uso de Bitcoin y otras herramientas digitales de manera segura para los usuarios, el gobierno ha empezado a implementar medidas como la aprobación de la política de ciberseguridad³⁵. Así, una implementación y socialización del marco regulatorio podría fortalecer la confianza y fomentar una mayor adopción de nuevas tecnologías en materia financiera³⁶,

A nivel mundial, El Salvador es visto favorablemente en lo que respecta a regulación de AV,³⁷ aunque ocupe la posición número 95 en términos de valor en transacciones a nivel global.³⁸ Este desempeño podría deberse en parte a la limitada alfabetización en materia financiera³⁹ y tecnológica para adoptar la tecnología y prevenir delitos financieros, así como retos operativos para el cumplimiento de las normas de seguridad de la información⁴⁰.

El Informe de Evaluación Mutua (EM) de El Salvador publicado en agosto de 2024, calificó la Reco-

²⁹ Instituto Universidad de Opinión Pública. (2024). Encuesta de evaluación del quinto año de Gobierno del presidente Nayib Bukele. <https://uca.edu.sv/iudop/wp-content/uploads/2024/06/PPT-Eva-5to-anio-de-NB-1.pdf>

³⁰ USAID. (2023). El Salvador Digital Ecosystem Country Assessment (DECA). <https://www.usaid.gov/digital-development/el-salvador-deca>.

³¹ USAID. (2023). pág. 50

³² Política Nacional de Inclusión Financiera para El Salvador (PNIF-SLV). Política Nacional de Inclusión Financiera para El Salvador

³³ Secretaría de Innovación de la Presidencia. (2020). El Salvador. agenda digital 2020-2030. <https://www.innovacion.gob.sv/downloads/Agenda%20Digital.pdf>.

³⁴ La Agenda Digital, liderada por la Secretaría de Innovación, se basa en cuatro pilares, entre los que destaca "Innovación, Educación y Competitividad", que incluye el área Fintech (finanzas y tecnología). El objetivo principal de esta iniciativa es promover la innovación en el sistema financiero mediante la creación de un marco regulatorio adecuado, el fomento de pasarelas de pago y la promoción de instrumentos financieros para la inclusión social. Secretaría de Innovación de la Presidencia. (s.f.). Fintech, <https://www.innovacion.gob.sv/fintech.php>.

³⁵ Secretaría de Innovación, Política de Ciberseguridad, 2021, <https://database.cyberpolicyportal.org/api/files/167683557209919pucn-6luha.pdf>

³⁶ Banco Mundial. (2022). Transformación Digital en El Salvador, reactivando el crecimiento y la inclusión. Transformación Digital en El Salvador, reactivando el crecimiento y la inclusión (bancomundial.org)

³⁷ Coincub. (2024). Crypto Regulation Report. https://x.com/coincub_/status/1803810784234852725?s=48.

³⁸ Chainalysis (2023). Geography of Cryptocurrency Report. <https://go.chainalysis.com/geography-of-cryptocurrency-2023.html>.

³⁹ Global Financial Integrity and Vance Center. (2023). The Virtual Assets Ecosystem In El Salvador: Strengthening Financial Integrity And Transparency. <https://gfintegrity.org/report/the-virtual-assets-ecosystem-in-el-salvador-strengthening-financial-integrity-and-transparency/>

⁴⁰ González, Glenda. Criptonoticias. (2024). Hackers filtran código de la Chivo Wallet de El Salvador. <https://www.criptonoticias.com/seguiridad-bitcoin/hackers-filtran-codigo-chivo-wallet-elsalvador/>

mendación 15⁴¹, relacionada con el uso de nuevas tecnologías incluyendo los activos virtuales, como parcialmente cumplida (PC)⁴². Es oportuno que El Salvador pueda incluir normativa pertinente para prevenir delitos financieros, en concordancia con el perfil del país en cuanto a capacidades, recursos y el uso de activos virtuales a nivel global.

MARCO NORMATIVO GENERAL SOBRE LA REGULACIÓN DE AV EN EL SALVADOR

En El Salvador, con la promulgación de la Ley Bitcoin (LB) en 2021⁴³ y la aprobación de la Ley de Emisión de Activos Digitales en 2023 (LEAD),⁴⁴ se estableció el marco regulatorio y jurídico para el uso del Bitcoin como moneda de curso legal y para las finanzas descentralizadas (DeFi). Además, se modificó la legislación penal sustantiva⁴⁵ para tipificar delitos relacionados con el uso ilícito de AV, específicamente aquellos cometidos contra los PSB/PSAD,

⁴¹ La recomendación 15 según GAFILAT consiste en que los países y las instituciones financieras deben identificar y evaluar los riesgos de lavado de activos o financiamiento del terrorismo que pudieran surgir con respecto a (a) el desarrollo de nuevos productos y nuevas prácticas comerciales, incluyendo nuevos mecanismos de envío, y (b) el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como los existentes, añadiendo que los países deben garantizar que los proveedores de servicios de activos virtuales estén regulados para propósitos ALA/CFT, y tengan licencia o registro y estén sujetos a sistemas de monitoreo efectivo y asegurar el cumplimiento de las medidas relevantes requeridos en las Recomendaciones del GAFI <https://biblioteca.gafilat.org/wp-content/uploads/2024/07/Recomendaciones-metodologia-act-DIC2023.pdf>, Página 16.

⁴² GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. Página 319. Informe de Evaluación Mutua de la República de El Salvador – GAFILAT

⁴³ Asamblea Legislativa. (2021). Ley de Emisión Activos Digitales. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/43DA8049-AA39-4DA8-B892-437B2DD27C1C.pdf>

⁴⁴ ídem

⁴⁵ Asamblea Legislativa. (2022). Decreto legislativo No. 236. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/6141982C-4614-4CF7-B658-D455A9A79616.pdf>

incluyendo daños a sistemas informáticos, fraude informático y el secuestro de sistemas, programas y datos informáticos. Estas normas, entre otras relacionadas, buscan fortalecer la seguridad jurídica y fomentar la confianza de la población en la tecnología; así como contrarrestar delitos financieros relacionados al uso de los activos virtuales.

Desde el 2021 hasta la fecha de publicación de este informe, se han aprobado y modificado alrededor de 20 regulaciones de diferente jerarquía en torno a los AV. Las mismas incluyen las reformas a la LEAD, que refuerzan la regla del viajero, proporcionan definiciones más claras sobre las monedas estables, eliminan algunos requisitos para la emisión de regulación y la unificación de la supervisión de los PSAD y PSB en un solo ente, la CNAD⁴⁶, así como la modificación de los requisitos para la factura electrónica en el Código Tributario⁴⁷. Varios reglamentos e instructivos especializados que regulan el Bitcoin, las monedas estables y la emisión de AD, como los activos subyacentes o referenciados han sido de igual forma aprobados y se han establecido lineamientos y guías de aplicación para los PSAV y PSB en materia ALA/CFT por parte de la UIF.

Asimismo, la Asamblea Legislativa se encuentra debatiendo distintos anteproyectos de ley (APL), entre los que se incluyen reformas a la Ley de Bancos para

⁴⁶ Hernández, Claudia. Global Financial Integrity. (2024). Cambios en la ley de activos digitales en El Salvador. <https://criptoabierto.com/cambios-en-la-ley-de-emision-de-activos-digitales-de-el-salvador/>

⁴⁷ Asamblea Legislativa. (2024). Decreto legislativo. 960 y 487 Reformas al código tributario. 9BA5E264-CE0D-4CA7-97D7-D8B-AC5CE106A.pdf (asamblea.gob.sv) A607DD05-7C5C-471B-A7F6-7393107250B7.pdf (asamblea.gob.sv)

incorporar la figura de bancos de inversión privada⁴⁸ y regular actividades con monedas estables.⁴⁹

Además, se estuvo evaluando una ley para la Prevención, Control y Sanción del Lavado de Activos, Financiamiento al Terrorismo y de la Proliferación de Armas de Destrucción Masiva que incorporaría a los PSAD/PSB como sujetos obligados.⁵⁰ Estas actualizaciones reflejan el esfuerzo continuo de El Salvador por adaptarse a las nuevas tecnologías, y garantizar su funcionamiento y fiabilidad, lo que representa desafíos en su aplicación efectiva.

MODIFICACIONES TRIBUTARIAS

En febrero de 2024 se aprobaron reformas al Código Tributario relacionadas con la factura electrónica y física para la identificación del comprador o prestador de servicios⁵¹. Dentro de las reformas, se contempla un incremento al umbral de transacciones, el cual era de US\$200.00 hasta US\$25,000 en relación a la identificación de la factura de consumidor final.⁵²

⁴⁸ Asamblea legislativa. (2024) Diputados estudian reformar ley para establecer banca privada de inversión en El Salvador. <https://www.asamblea.gob.sv/node/13220>

⁴⁹ Magaña, Yolanda. Diario El Mundo. (2024). El Salvador crearía bancos privados de inversión para clientes con activos libres desde \$250,000. <https://diario.elmundo.sv/politica/el-salvador-crearia-bancos-privados-de-inversion-para-clientes-con-activos-libres-desde-250000>

⁵⁰ Fiscalía General de la República. (2023). Aprobación de la Ley Especial para la Prevención, Control y Sanción del LA/FT y de la Proliferación de Armas de Destrucción Masiva <https://www.uif.gob.sv/aprobacion-de-la-ley-especial-para-la-prevencion-control-y-sancion-del-la-ft-y-de-la-proliferacion-de-armas-de-destruccion-masiva/>

⁵¹ Asamblea Legislativa. (2024). Decreto legislativo. 960 reformas al código tributario. 9BA5E264-CE0D-4CA7-97D7-D8BAC5CE106A.pdf (asamblea.gob.sv)

⁵² ídem.

En este mismo sentido, en marzo de 2024 la Ley del Impuesto sobre la Renta, fue modificado en el artículo 3, para eximir de pago a cualquier valor recibido bajo cualquier concepto en el extranjero, así como cualquier movimiento de capital, remuneración o emolumento, en dinero o en especie, generado por la inversión de capital nacional o extranjero. Esto aplica a personas naturales, entidades jurídicas o entidades sin personalidad jurídica, ya sea que se encuentren dentro o fuera de El Salvador. No obstante, esta exención se limita a ingresos generados fuera del país; los ingresos obtenidos dentro de El Salvador continúan sujetos al pago de Impuesto sobre la Renta correspondiente.⁵³

Adicionalmente, entre los meses de agosto y septiembre de 2024, el Ministerio de Hacienda publicó una circular en la que se establece que, en las ventas realizadas por consumidores finales en operaciones menores de US\$25,000, no es necesario solicitar datos personales como el número de identificación, correo electrónico, número móvil y actividad económica⁵⁴. Por otra parte, la UIF indicó que, para el sector comercial, las políticas de debida diligencia del cliente (DDC) deben ser aplicadas únicamente para transacciones en efectivo superiores a los US\$10,000 o transacciones superiores a los US\$25,000 a través de cualquier

⁵³ Asamblea Legislativa. (2024). Decreto legislativo. 969 reformas a la ley de impuesto sobre la renta. 86A64E36-EB7C-4F57-82BC-A289A5D94C33.pdf (asamblea.gob.sv)

⁵⁴ The Bitcoin Office. [@bitcoinofficesv]. (2024). Regarding the demands for identification cards some have encountered in shops in El Salvador on purchases of less than \$25,000, please read the notice below from the Ministry of Finance. [Mensaje en X]. <https://x.com/bitcoinofficesv/status/1831534362841465183?s=46>

otro medio de pago⁵⁵. La UIF excluyó a las instituciones financieras, a las actividades y profesiones no financieras designadas (APNFD), los PSB y PSAD en la aplicación de esta medida, por lo que, estos sectores estarían obligados a realizar la DDC para las transacciones menores de US\$25,000⁵⁶.

Finalmente, el 17 de septiembre de 2024, la Asamblea Legislativa aprobó otra reforma al Código Tributario que impone una multa por la exigencia indebida de datos personales a personas naturales, nacionales o extranjeras, que adquieran bienes y/o servicios por un monto inferior a US\$25,000⁵⁷.

Se exceptúan aquellos casos en que las personas naturales necesiten una factura para documentar la operación o requieran deducir el gasto, en cuyo caso, si son extranjeros, deberán presentar un documento fiscal del país de su domicilio. En el caso de las personas jurídicas, será necesario siempre indicar la denominación social, independientemente del monto⁵⁸. Si se requiere documentar la operación o deducir el gasto, la persona jurídica deberá proporcionar el número de identificación tributaria y, si es extranjera, su número de registro fiscal del país de su domicilio u otro documento que pueda identificarla.

⁵⁵ Fiscalía General de la República. [@FGR_SV] (2024). La @FGR a través de la unidad de investigación financiera comunica lo siguiente: [post X] Fiscalía General de la República El Salvador on X: "¡ATENCIÓN! 📢 La @FGR_SV a través de la Unidad de Investigación Financiera comunica lo siguiente: Los Sujetos Obligados con Actividades no financieras que realicen transacciones inferiores a los \$10,000 dólares en efectivo o superiores a \$25,000 dólares en otras formas de <https://t.co/srPjVEFUml>" / X

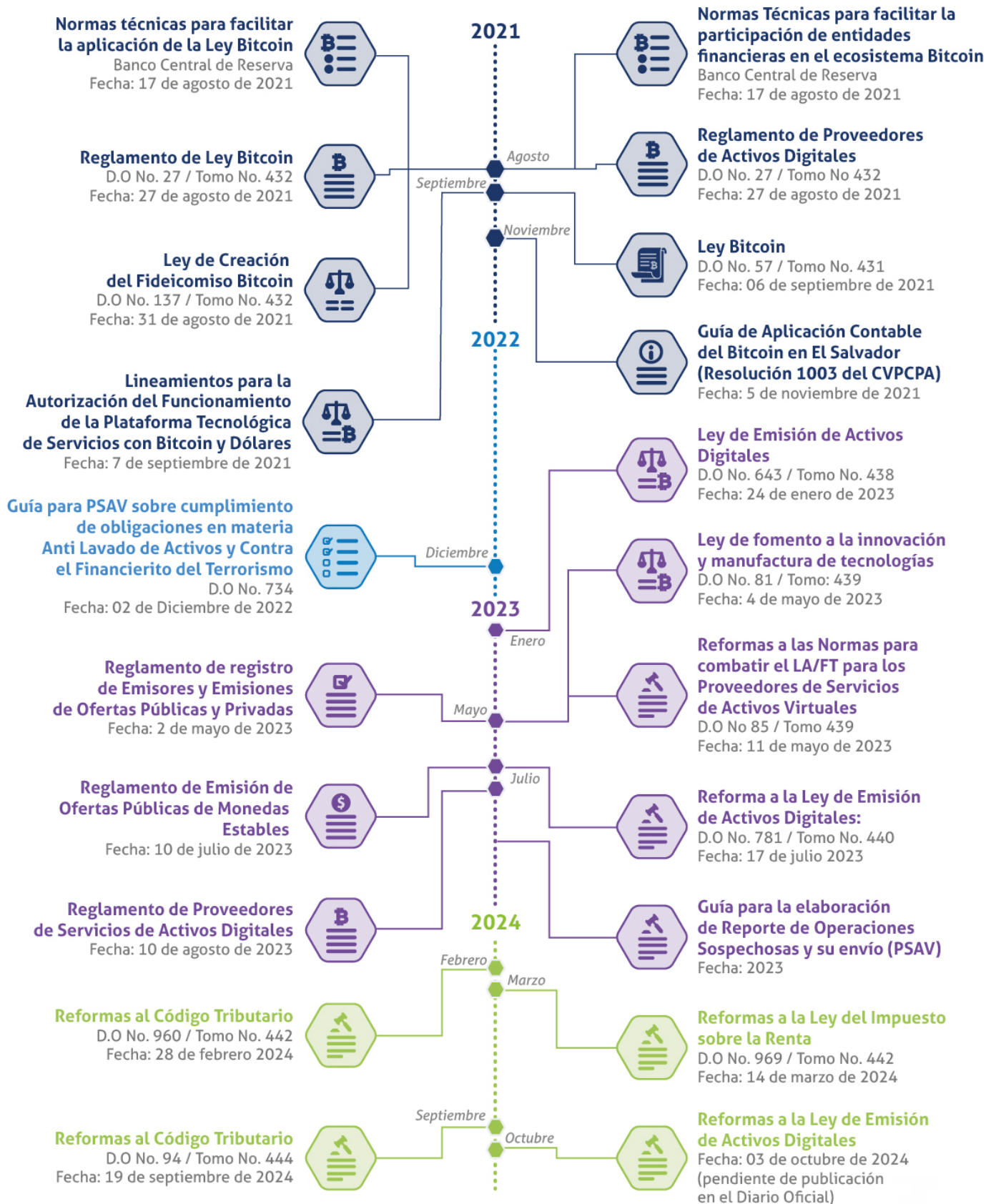
⁵⁶ Ídem.

⁵⁷ Asamblea Legislativa. [@AsambleaSv] (2024). Con 57, votos a favor, reformamos el código tributario, con el fin de simplificar y maximizar la aplicación de los documentos tributarios, tanto físicos como electrónicos. [post X] <https://x.com/asambleasv/status/1836186287247630387?s=46>

⁵⁸ Ídem.

Gráfico 1

CRONOLOGÍA DE LA REGULACIÓN DE LOS ACTIVOS VIRTUALES EN EL SALVADOR



PANORAMA GENERAL DE INVERSIÓN EN BITCOIN DEL GOBIERNO DE EL SALVADOR

Las primeras compras de Bitcoin por parte del GOES, se realizaron el 6 de septiembre de 2021 contabilizando once⁵⁹ compras de Bitcoin. Estas compras hacen un total de ₡2,381 bitcoins hasta el día 16 de noviembre de 2022, cuando se anunció por la red social "X", la decisión de comprar 1 BTC al día a partir del siguiente día.

El 17 de noviembre de 2022 se inició con la compra de 1 BTC al día⁶⁰, contabilizando hasta el día 14 de marzo de 2024⁶¹, fecha en la que se publicó la dirección de la billetera fría del Gobierno de El Salvador, la cantidad de ₡2,865 bitcoins en total⁶².

El 14 de marzo de 2024, fecha en la cual, el presidente de El Salvador dio a conocer la dirección de la

billetera fría⁶³ a través de la red social "X" del GOES (32ixEdVJWo3kmvJGMTZq5jAQVZZeuwnqzo⁶⁴), el balance general publicado de la billetera fría reflejaba la cantidad de ₡5,689.68509200 bitcoins⁶⁵, equivalentes en esa fecha a US \$406,607,655.⁶⁶

Asimismo, en esa misma publicación, el presidente anunció que esta nueva billetera estaría resguardada en una "bóveda física dentro de nuestro territorio nacional".⁶⁷

El 12 de mayo de 2024, la Oficina Nacional del Bitcoin (ONBTC) publicó⁶⁸ en su sitio web una herramienta "Bitcoin Explorer" que permite transparen-

⁵⁹ 1. <https://x.com/nayibbukele/status/143496847592824833>
2. <https://x.com/nayibbukele/status/1435023474494410753>
3. <https://x.com/nayibbukele/status/1435260422110732300>
4. <https://x.com/nayibbukele/status/1439815012642611203>
5. <https://x.com/nayibbukele/status/1453461587948445697>
6. <https://x.com/nayibbukele/status/1464307422793715716>
7. <https://x.com/nayibbukele/status/1467000621354135555>
8. <https://x.com/nayibbukele/status/1473489844521385985>
9. <https://x.com/nayibbukele/status/1484651539587289091>
10. <https://x.com/nayibbukele/status/1523742670044413954>
11. <https://x.com/nayibbukele/status/1542672286490271744>

⁶⁰ Bukele, N. [@nayibbukele]. (2022) We are buying one #Bitcoin every day starting tomorrow. Mensaje en X]. <https://x.com/nayibbukele/status/1593113857261965312>

⁶¹ Bukele, N. [@nayibbukele]. (2024). We've decided to transfer a big chunk of our #Bitcoin to a cold wallet, and store that cold wallet in a physical vault within our national territory [Mensaje en X]. <https://x.com/nayibbukele/status/1768425845163503738?s=48>

⁶² A= 11 compras de Bitcoin realizadas entre el 06 de septiembre de 2021 y el 16 de noviembre de 2022, conforme a las publicaciones realizadas en la plataforma X: ₡2,381 bitcoins
B= días transcurridos entre el 17 de noviembre y el 14 de marzo de 2024, haciendo un total de 484 días, que bajo la decisión de compra de 1 BTC al día contabilizaría la cantidad de: ₡484
A+B=₡2,865 bitcoins.

⁶³ Una billetera fría es un dispositivo hardware que almacena criptomonedas, y que no se encuentra conectado a internet. Coinbase. Cartera de criptoactivos caliente vs fría: ¿cuál es la diferencia? <https://www.coinbase.com/es-es/learn/wallet/hot-vs-cold-crypto-wallet-what-is-the-difference#:~:text=Las%20carteras%20fr%C3%A4Das%20son%20basadas,las%20necesidades%20y%20preferencias%20individuales>.

⁶⁴ Bukele, N. [@nayibbukele]. (2024). We've decided to transfer a big chunk of our #Bitcoin to a cold wallet, and store that cold wallet in a physical vault within our national territory [Mensaje en X]. <https://x.com/nayibbukele/status/1768425845163503738?s=48>.

⁶⁵ Transacción 1: <https://mempool.space/tx/130c87cb615456ca8f-126c502068e53e481611cb42fed248da560f6e01d1fe6a>
Transacción 2: <https://mempool.space/tx/4d7ee580190b1aadd-4603a5953ef385c5c06b531dc62d1229f5ea87c379b69da>,
Transacción 3: <https://mempool.space/tx/3870a2d9fad1328c-dadb2a7ea2344191d1a507d933de7de115144fdef74427f9>,
Transacción 4: <https://mempool.space/tx/968d0b0f6c697668f-9ca04a4904ed9a3629c20b11e470392510629a32eddeb03>,
Transacción 5: <https://mempool.space/tx/24bd78028879ed7fbd-159fcbe16855a506ef46f0b69f9239a201fcc054775f52>,
Transacción 6: <https://mempool.space/tx/6005f0d2a6494501f2bd-c47ae05de749d5fa08042c28dd7db664ae51344f3904>

⁶⁶ El precio del Bitcoin al 14 de marzo de 2024 es de US\$69,463.7 <https://es.investing.com/crypto/bitcoin/historical-data>

⁶⁷ Bukele, N. [@nayibbukele]. (2024). We've decided to transfer a big chunk of our #Bitcoin to a cold wallet, and store that cold wallet in a physical vault within our national territory [Mensaje en X]. <https://x.com/nayibbukele/status/1768425845163503738?s=48>.

⁶⁸ The Bitcoin Office. El Salvador. (s.f.). <https://x.com/bitcoinofficesv/status/1789788632070431046>.

tar la trazabilidad de la dirección del GOES⁶⁹, sobre todo la compra de 1 BTC al día⁷⁰. Esta herramienta de trazabilidad es similar a otras herramientas de fuentes abiertas, que contienen un buscador para rastrear direcciones de BTC, bloques y hashes de transacciones dentro de la cadena de bloques o Blockchain de Bitcoin⁷¹.

Hasta la fecha de cierre de este informe, el día 8 de octubre de 2024, verificando el balance general de la dirección del GOES, se contabilizaba la cantidad de ₡5,896.75942931 bitcoins equivalentes a US\$370,458,014.⁷²

⁶⁹ Conforme a las herramientas de fuentes abiertas la primera transacción de la dirección del GOES data el día 13 de marzo de 2024: <https://glasschain.org/btc/Address/32ixEdVJWo3kmvJGMTZq5jAQVZZeuwnqzo>

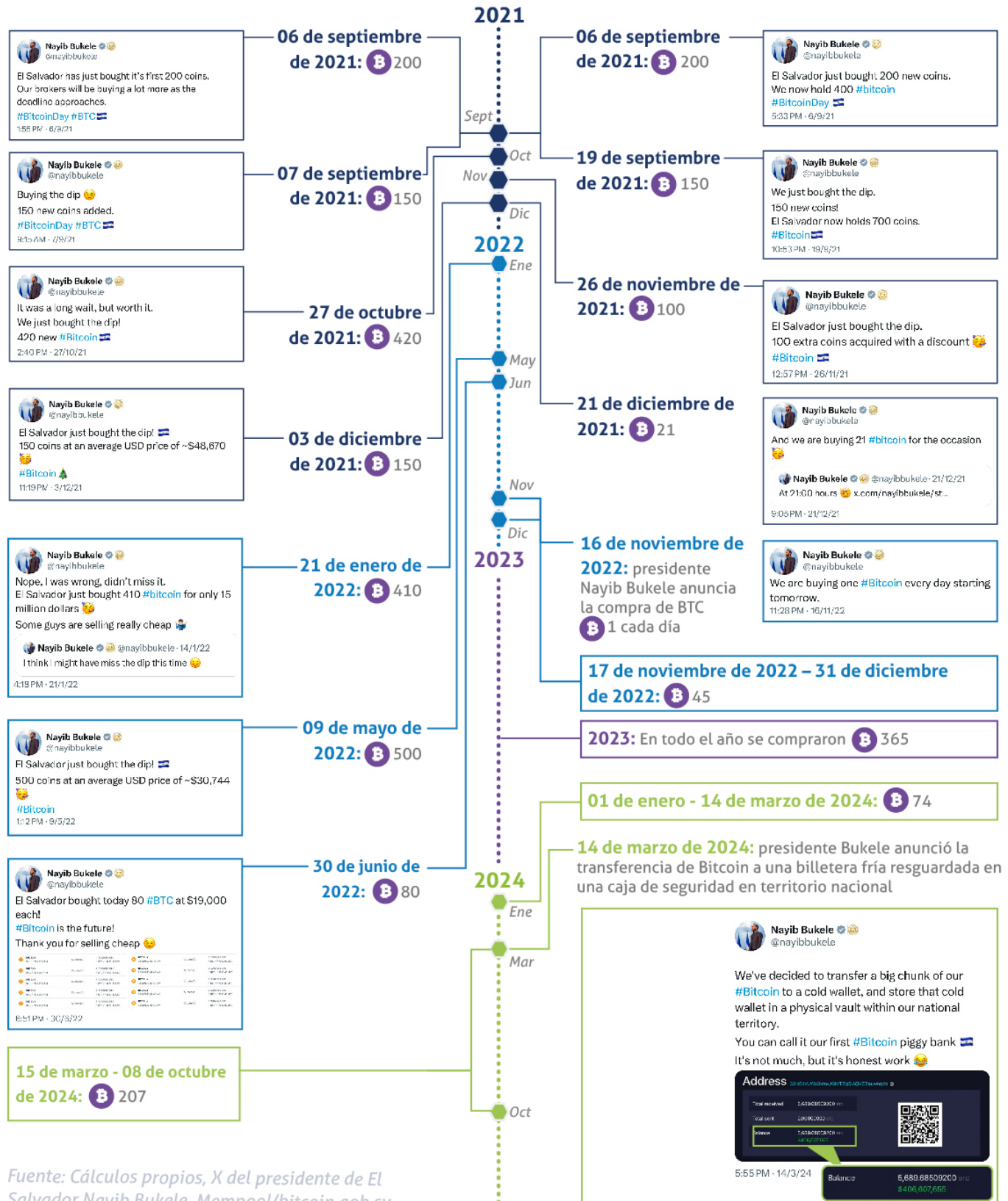
⁷⁰ El 17 de noviembre de 2022, el presidente Bukele publicó en la red social X (antiguo Twitter) que, a partir del día siguiente, el 18 de noviembre de 2022, el gobierno compraría ₡1 al día. Desde el 18 de noviembre de 2022 hasta el 30 de abril de 2023, el gobierno compró ₡164.

⁷¹ Mempool Space, <https://mempool.space/address/32ixEdVJWo3kmvJGMTZq5jAQVZZeuwnqzo>. Blockchair, <https://blockchair.com/bitcoin/address/32ixEdVJWo3kmvJGMTZq5jAQVZZeuwnqzo>. Blockchain.info <https://www.blockchain.com/explorer/addresses/btc/32ixEdVJWo3kmvJGMTZq5jAQVZZeuwnqzo>

⁷² El precio del Bitcoin al 8 de octubre 2024 es de US\$62,673.05 <https://coinmarketcap.com/currencies/bitcoin/>

Gráfico 2

COMPRAS DE BITCOIN DEL GOBIERNO DE EL SALVADOR: ANÁLISIS DE PUBLICACIONES EN REDES SOCIALES Y BITCOIN BLOCKCHAIN



Fuente: Cálculos propios, X del presidente de El Salvador Nayib Bukele, Mempool/bitcoin.gob.sv

El resguardo de las claves de acceso a la billetera fría debe ser extremadamente cuidadosa⁷³, ya que al igual que las billeteras calientes, las billeteras frías, a pesar de no estar conectadas a internet, presentan retos de seguridad de la información. La billetera fría del GOES estaría resguardando 5,896.75942931⁷⁴ bitcoins equivalentes a US\$370,458,014⁷⁵ conforme al balance general de la misma dirección.

⁷³ Alexander, Doug. The Seattle Times. (2019). Crypto CEO dies holding the only passwords that can unlock millions in customer coins. <https://www.seattletimes.com/business/crypto-ceo-dies-holding-only-passwords-that-can-unlock-millions-in-customer-coins/>.

⁷⁴ Cantidad de Bitcoins al 8 de octubre de 2024.

⁷⁵ El precio del Bitcoin al 8 de octubre 2024 es de US\$62,673.05 <https://coinmarketcap.com/currencies/bitcoin/>

1

CAPÍTULO 1

Marco legal para la prevención del lavado de dinero y activos en El Salvador: Aspectos generales de la ley vigente y anteproyecto de ley en debate



El marco normativo institucional y normativo para la prevención del LD y LA en El Salvador se rige por la Ley Contra el Lavado de Dinero y Activos de 1998, cuyo objetivo es “prevenir, detectar, sancionar y erradicar el delito de lavado de dinero y activos y su encubrimiento”⁷⁶. Dentro de ella se encuentra un listado de veinte sujetos obligados⁷⁷, quienes tienen la obligación de reportar las diligencias u operaciones financieras sospechosas o que superen el umbral de la ley, así como el de capacitar a una persona designada como oficial de cumplimiento. Las instituciones intervinientes contemplan principalmente a la Unidad de Investigación Financiera (UIF), la cual se desarrollará más adelante⁷⁸.

El marco normativo de ALA/CFT ha sido abordado recientemente a raíz de los resultados de la evaluación mutua (EM) realizada por el GAFILAT tras la vi-

⁷⁶ Asamblea Legislativa. Ley contra el lavado de dinero y activos (1998), decreto 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0B869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

⁷⁷ Los sujetos obligados de la Ley Contra el Lavado de Dinero y Activos de 1998, comprenden a: a) toda sociedad, empresa o entidad de cualquier tipo, nacional o extranjera, que integre una institución, grupo o conglomerado financiero supervisado y regulado por la superintendencia del sistema financiero; b) micro-financieras, cajas de crédito e intermediarias financieras no bancarias; c) importadores o exportadores de productos e insumos agropecuarios, y de vehículos nuevos o usados; d) importadores o exportadores de productos e insumos agropecuarios, y de vehículos nuevos o usados; e) personas naturales y jurídicas que realicen transferencias sistemáticas o sustanciales de fondos, incluidas las casas de empeño y demás que otorgan préstamos; f) casinos y casas de juego; g) comercializadores de metales y piedras preciosas; h) empresas e intermediarios de bienes raíces; i) agencias de viajes, empresas de transporte aéreo, terrestre y marítimo; j) personas naturales y jurídicas que se dediquen al envío y recepción de encomiendas y remesas; k) empresas constructoras; l) empresas privadas de seguridad e importadoras y comercializadoras de armas de fuego, municiones, explosivos y artículos similares; m) empresas hoteleras; n) partidos políticos; ñ) proveedores de servicios societarios y fideicomisos; o) organizaciones no gubernamentales; p) inversionistas nacionales e internacionales; q) droguerías, laboratorios farmacéuticos y cadenas de farmacias; r) asociaciones, consorcios y gremios empresariales; s) cualquier otra institución privada o de economía mixta, y sociedades mercantiles; así como los abogados, notarios, contadores y auditores.

⁷⁸ Asamblea Legislativa. Ley contra el lavado de dinero y activos (1998), decreto 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0B869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

sita in situ en enero de 2024.⁷⁹ La importancia de la EM radica en su capacidad de identificar áreas clave de mejora que el país debe adoptar para fortalecer su sistema preventivo. El Salvador destaca como uno de los pocos países en la región que ha regulado los AV, y además, es pionero en adoptar el Bitcoin como moneda de curso legal. En este sentido es importante prevenir un posible aumento en la incidencia de riesgos asociados al uso de AV.⁸⁰

En relación al FT, la EM ha destacado que El Salvador ha concentrado sus esfuerzos principalmente en la clasificación de pandillas y maras como grupos terroristas locales, cuyos actos suelen financiarse a través de delitos determinantes.⁸¹ Sin embargo, sería importante realizar un análisis sobre los riesgos potenciales del FT y el uso de AV por parte de organizaciones terroristas. Sin ello, podría limitar el alcance del país en la identificación y mitigación de los riesgos relacionados con este fenómeno criminal.⁸²

A. MARCO NORMATIVO

La Ley Contra el Lavado de Dinero y Activos (LCLDA) vigente (1998) y su reglamento han sido hasta la fecha la normativa principal sobre la materia y bajo las cuales se han desarrollado las actividades de las instituciones involucradas y los sujetos obligados. Han existido diversas iniciativas para reformar

⁷⁹ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. Informe de Evaluación Mutua de la República de El Salvador – GAFILAT.

⁸⁰ GAFILAT. (2024) (pág. 22, pár. 29).

⁸¹ GAFILAT. (2024) pág. 22, pár. 30).

⁸² GAFILAT. (2024) pág. 22, pár. 31).

la LCLDA y una interpretación auténtica, desde 1998 hasta el año 2013⁸³. Adicionalmente, se creó un anteproyecto de ley en el año 2018, el cual fue archivado⁸⁴. No fue hasta el año 2023, que se presentó un anteproyecto de ley (incluido en el estudio de este informe) el cual tiene como objetivo realizar cambios significativos dentro del marco normativo e institucional en materia de prevención ALA/CFT, como más adelante se explica.

LEY CONTRA EL LAVADO DE DINERO Y ACTIVOS (LCLDA) VIGENTE (1998)

La Ley LCLDA es el marco jurídico principal para el combate al LA/FT cuyo objetivo principal es “prevenir, detectar, sancionar y erradicar el delito de lavado de dinero y su encubrimiento”⁸⁵. La ley regula las obligaciones de los sujetos obligados (SO), así como el rol de los supervisores y de la Unidad de Inteligencia Financiera (UIF).

El alcance de los SO incluye un amplio número de actividades financieras, comerciales y profesionales, estableciendo los delitos subyacentes al lavado de dinero y regula el delito en sí, junto a otros conexos⁸⁶. Entre los aspectos más destacados del marco normativo se encuentra la obligación de reportar operaciones sospechosas y la aplicación de

medidas de debida diligencia reforzada, especialmente para clientes de alto riesgo y para las personas políticamente expuestas (PEP)⁸⁷. Además, la normativa exige la conservación de los documentos del cliente y establece que los oficiales de cumplimiento realicen seguimientos rutinarios para detectar operaciones inusuales⁸⁸.

Adicionalmente, la LCLDA y otros documentos emitidos por la UIF establecen que los SO tienen la obligación de inscribirse en la plataforma de la UIF⁸⁹ para reportar las operaciones sospechosas. Asimismo, deben inscribir al oficial de cumplimiento y su suplente,⁹⁰ remitiendo la documentación que acredite: a) la creación de la Oficialía de Cumplimiento, b) la designación del responsable de cumplimiento, c) el manual de cumplimiento para la prevención de LA/FT, d) un documento explicativo del sistema de análisis de alertas, e) un plan de auditoría.⁹¹

⁸³ Asamblea Legislativa. Ley contra el lavado de dinero y activos (1998), decreto 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0B869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

⁸⁴ El Diario de Hoy, Fiscalía presenta a diputados propuesta de ley para el combate al lavado de dinero y activos. (2018). <https://historico.elsalvador.com/historico/534461/fiscal-general-presenta-reformas-a-ley-de-lavado-de-dinero-que-aumenta-las-penas-menores-de-cinco-a-ocho-anos.html>

⁸⁵ ídem.

⁸⁶ ídem

⁸⁷ ídem

⁸⁸ ídem

⁸⁹ Fiscalía General de la República. (2021). Instructivo de la unidad de investigación financiera para la prevención del lavado de dinero y de activos, fiscalía general de la república. <https://www.uif.gob.sv/wp-content/uploads/instructivos/InstructivoUifDiarioOficial2021.pdf>.

⁹⁰ Fiscalía General de la República. (2021).

⁹¹ Fiscalía General de la República. (2021)

ANTEPROYECTO LEY ESPECIAL PARA LA PREVENCIÓN, CONTROL Y SANCIÓN DEL LAVADO DE ACTIVOS, FINANCIAMIENTO AL TERRORISMO Y DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA DE 2023 (APL)

A finales del año 2023,⁹² el Ministro de Justicia y Seguridad presentó a la Asamblea Legislativa un nuevo APL que busca reformar la actual ley y cumplir con los estándares establecidos por GAFI y GAFILAT. Al momento de cierre de este informe, el APL continúa en discusión en la Comisión de Seguridad Pública y Combate a la Narcoactividad. A continuación, se presentan algunos puntos relevantes del anteproyecto:

• Sistema Nacional para la Prevención, Control y Represión del LA/FT/PADM.

El APL de 2023 propone la creación del Sistema Nacional para la Prevención, Control y Represión del LA/FT, el cual coordinará de manera conjunta a las entidades que lo integren⁹³. Este sistema estaría compuesto por la Fiscalía General de la República, entidades de fiscalización, supervisión, regulación y vigilancia en la materia, así como los SO. El objetivo principal es centralizar y optimizar el intercambio de información y la coordinación de operaciones entre entidades, mejorando así la capacidad de detección y combate de actividades ilícitas.

• Comité Interinstitucional para la Prevención del Lavado de Activos y Financiación del Terrorismo (CIPLAFT).

El CIPLAFT actuaría como un organismo consultivo y de coordinación estratégica, encargado de diseñar y proponer al Órgano Ejecutivo las políticas, estrategias y planes de acción para la prevención, detección y combate de LA/FT⁹⁴. Estaría conformado por: a) la Fiscalía General de la República, que presidiría el CIPLAFT; b) el presidente de la Corte Suprema de Justicia; c) el Ministro de Justicia y Seguridad Pública; d) Ministro de Hacienda; e) el ministro de la Defensa Nacional; f) el Ministro de Economía; g) el presidente del Banco Central de Reserva; y h) el Superintendente del Sistema Financiero⁹⁵.

Entre sus facultades, el CIPLAFT tendría la potestad de incluir o eliminar SO de la regulación. Para ello, es fundamental definir y hacer transparentes los criterios bajo los cuales se decidiría la inclusión o exclusión de los SO.

⁹² Asamblea Legislativa [@AsambleaSV]. (2024). Los diputados emiten dictamen favorable a las siguientes iniciativas: Aprobación de la Ley Especial para la Prevención, Control y Sanción del Lavado de Activos, Financiamiento al Terrorismo y de la Proliferación de Armas de Destrucción Masiva. [post X]. <https://x.com/AsambleaSV/status/>

⁹³ Asamblea Legislativa. Anteproyecto de Ley Ley Especial para la Prevención, Control y Sanción del Lavado de Activos, Financiamiento al Terrorismo y de la Proliferación de Armas de Destrucción Masiva, (2023), Título II.

⁹⁴ ídem

⁹⁵ ídem

LEY DE EMISIÓN DE ACTIVOS DIGITALES Y SUS REFORMAS: Registro, Reguladores, Supervisores y Entes Sancionadores de PSAD

Para los AV, el GAFI recomienda que los países establezcan regulaciones para prevenir actividades relacionadas con el LA/FT⁹⁶. En El Salvador, el ecosistema de AV se clasificaba en dos hasta las reformas aprobadas el 3 de octubre de 2024 de la Ley de Emisión de Activos Digitales (LEAD)⁹⁷. Antes de esa reforma los PSB, el registro y licenciamiento estaban a cargo del Banco Central de Reserva (BCR),⁹⁸ quien era responsable de crear el registro y regular a los PSB de acuerdo con la LB, su reglamento y demás normativa. Y, la Superintendencia del Sistema Financiero (SSF)⁹⁹ estaba a cargo de la supervisión ejerciendo las mismas facultades que aplica sobre el sistema financiero tradicional.

A partir de la reforma, la Comisión Nacional de Activos Digitales (CNAD) se encarga del registro relacionado con los activos digitales (AD),¹⁰⁰ emiso-

res,¹⁰¹ certificadores,¹⁰² PSAD,¹⁰³ y emisiones de AD.¹⁰⁴ También supervisa y sanciona a los sectores registrados que no cumplen con la normativa aplicable.¹⁰⁵ Con la actual reforma de la LEAD, la CNAD también se encuentra a cargo de llevar el registro, regular, supervisar y sancionar a los PSB, y ya no corresponde al BCR ni a la Superintendencia ejercer las funciones habilitadas para ello.

La reforma de la LEAD ha buscado simplificar el ecosistema de los activos digitales, colocando a un mismo ente regulador, supervisor y sancionador para los PSB y PSAD, a pesar de la complejidad del sistema financiero digital y de cumplimiento, para la aplicación Recomendación 15 del GAFI.

⁹⁶ GAFI, Recomendación 15, <https://biblioteca.gafilat.org/wp-content/uploads/2024/07/Recomendaciones-metodologia-act-DIC2023.pdf>,

⁹⁷ Asamblea Legislativa. (2023). Reforma a la Ley de Activos Digitales. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/DA8F5A99-0267-4830-AA47-D03C37413608.pdf>

⁹⁸ Banco Central de Reserva de El Salvador. (s.f). Registro de Proveedores de Servicios Bitcoin. <https://registrobotcoin.bcr.gob.sv/web/inicio>

⁹⁹ Ministerio de Economía. (2021). Reglamento de la Ley Bitcoin. (Art.5), <https://www.iscpeelsalvador.org/wp-content/uploads/Reglamento-Ley-Bitcoin.pdf>

¹⁰⁰ Comisión Nacional de Activos Digitales. (s.f). Registro público <https://cnad.gob.sv/public-registry/>

¹⁰¹ Comisión Nacional de Activos Digitales. (s.f). Lista de emisores. <https://cnad.gob.sv/issuers/>

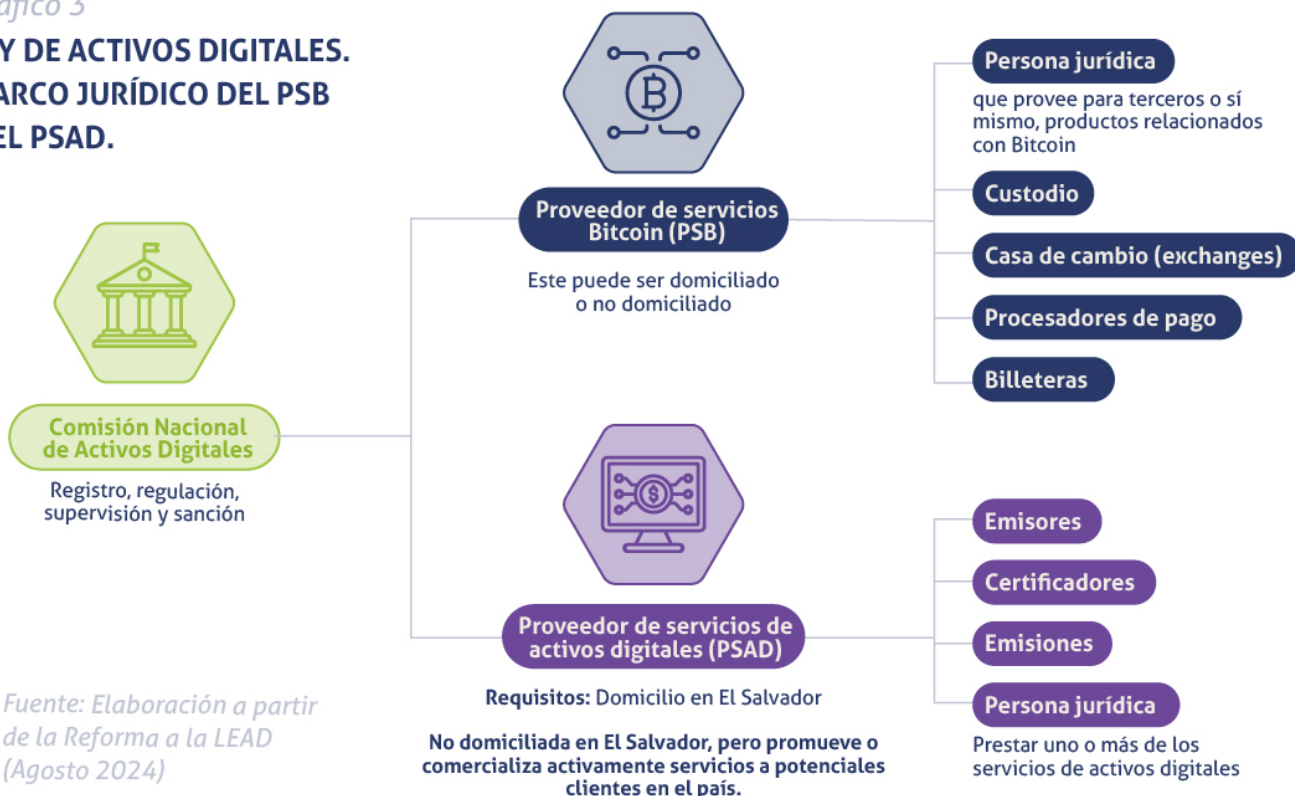
¹⁰² Comisión Nacional de Activos Digitales. (s.f). Lista de certificadores. <https://cnad.gob.sv/certifiers/>

¹⁰³ Comisión Nacional de Activos Digitales. (s.f). PSAD. <https://cnad.gob.sv/public-registry/digital-assets-service-provider/>

¹⁰⁴ Comisión Nacional de Activos Digitales. (s.f). Lista de emisores. <https://cnad.gob.sv/issuances/>

¹⁰⁵ Asamblea Legislativa. (2023). Ley de emisión de activos digitales. <https://www.asamblea.gob.sv/sites/default/files/documents/dictámenes/7050D57B-97A1-492F-AA15-CFCAEEF6E138.pdf>

Gráfico 3
LEY DE ACTIVOS DIGITALES.
MARCO JURÍDICO DEL PSB
Y EL PSAD.



B. MARCO INSTITUCIONAL

A continuación se detalla brevemente algunas facultades de la UIF dentro del marco normativo actual, así como su función para el cumplimiento de los estándares GAFILAT, entre los que se mencionan a los reportes de operaciones sospechosas, la debida diligencia del cliente, las personas políticamente expuestas, los beneficiarios finales, y los sujetos obligados. Ello haciendo una comparación con la legislación vigente y el APL, el cual contempla la incorporación de otros sujetos obligados como los proveedores de servicios de activos virtuales.

UNIDAD DE INVESTIGACIÓN FINANCIERA (UIF)

La vigente Ley Contra el Lavado de Dinero y Activos (LCLDA) establece que la UIF es una oficina adscrita a la Fiscalía General de la República (FGR) encargada de la investigación del Delito de Lavado de Dinero y de Activos¹⁰⁶, con autonomía funcional y técnica, cuya estructura organizativa está determinada por la

¹⁰⁶ Asamblea Legislativa. Ley Orgánica de la Fiscalía General de la República (2006), decreto 1037. <https://www.fiscalia.gob.sv/wp-content/uploads/portal-transparencia/leyes/ley-organica-FGR.pdf>

Ley Orgánica de la FGR¹⁰⁷. La UIF es el único centro nacional encargado de recibir y analizar los Reportes de Operaciones Sospechosas (ROS), así como de cualquier información relacionada con el LA/FT¹⁰⁸.

La capacidad de la UIF para actuar como el único centro de análisis y recepción de información financiera refuerza su papel en la estrategia nacional contra el LA/FT/PDAM¹⁰⁹.

REPORTES DE OPERACIONES SOSPECHOSAS (ROS)

La Recomendación 20 del GAFI y su nota interpretativa establecen la obligación de las instituciones financieras de reportar las operaciones sospechosas, ya sea porque existe una sospecha de que los fondos provienen de una actividad delictiva o que están relacionados con el FT.¹¹⁰ En la LCLDA, la obligación de reportar se extiende a las actividades y profesiones no financieras designadas (APNFD), como abogados, notarios, contadores y auditores.

En la LCLDA vigente, los ROS deben hacerse en un plazo de cinco días hábiles desde que se realice un análisis y determine que son irregulares¹¹¹. El

APL por el contrario, sugiere un plazo expedito de 24 horas para informar ROS después de haber finalizado el análisis respectivo, y existan suficientes elementos para considerar la operación como sospechosa. El cumplimiento riguroso de las obligaciones de reportar operaciones sospechosas es esencial para la integridad del sistema financiero y la prevención LA/FT. En este punto, la UIF juega un papel crucial al proporcionar las herramientas y el marco legal necesarios para que los sujetos obligados identifiquen y reporten las actividades sospechosas de manera oportuna y precisa.

DEBIDA DILIGENCIA DEL CLIENTE (DDC)

La Recomendación 10 del GAFI establece que las instituciones financieras realicen la DDC para eliminar cuentas anónimas o ficticias y que éstas garanticen que la información esté debidamente verificada para cada uno de los clientes. Para llevar a cabo lo anterior, debe establecerse una política interna de debida diligencia, la que debe incluir: la identificación y verificación del cliente (persona natural o jurídica), el beneficiario final (BF), el propósito y naturaleza de la relación comercial, y el monitoreo continuo.¹¹²

¹⁰⁷ ídem

¹⁰⁸ Asamblea Legislativa. Ley contra el lavado de dinero y activos (1998), decreto 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0B869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

¹⁰⁹ ídem

¹¹⁰ Financial Action Task Force. (2023). International Standards on combating ML/TF/PF. [https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf](https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf)

¹¹¹ Art. 9 de la Ley Contra el Lavado de Dinero y Activos (LCLDA) <https://ssf.gob.sv/wp-content/uploads/2022/07/Ley-contra-el-lavado-de-dinero-y-de-Activos-D498.pdf>

¹¹² CFATF-GAFIC.(s.f.) 40 Recomendaciones del GAFI. RECOMENDACIÓN 10. Debida diligencia del cliente (cfatf-gafic.org)

Cuando se trata de personas jurídicas, las instituciones financieras deben identificar y verificar al cliente, comprender la actividad comercial, para poder evaluar los riesgos potenciales del negocio, así como la estructura, titularidad y control¹¹³.

Estas medidas de DDC deben ser implementadas utilizando un enfoque basado en riesgos (EBR), lo que significa que, cuando existan riesgos mayores, las instituciones deberán aplicar medidas intensificadas para administrar y mitigar los riesgos, y cuando los riesgos sean menores, pueden permitirse la aplicación de medidas simplificadas.¹¹⁴

PERSONAS POLÍTICAMENTE EXPUESTAS (PEP)

Es pertinente contar con una lista explícita de personas consideradas como las personas políticamente expuestas (PEP), facilitando la identificación y el cumplimiento de las regulaciones pertinentes. Para definir quiénes son las PEP, la ley vigente remite a la Constitución de la República y a la Convención de las Naciones Unidas Contra la Corrupción. Por tanto, se consideran PEP a los funcionarios que ejercen los cargos públicos de más alto nivel, ya sea de elección popular, nombramiento o designación¹¹⁵. Además, cualquier otro funcionario público que cumpla con los criterios establecidos en la Convención de las Naciones Unidas contra la Corrupción (CNUCC), será considerado PEP. Espe-

cíficamente, aquellos que: a) ocupen un cargo legislativo, ejecutivo, administrativo o judicial de un Estado parte de la CNUCC, ya sea designado o elegido, permanente o temporal, remunerado u honorario, sin importar su antigüedad en el cargo; b) desempeñe una función pública, incluso para un organismo o una empresa pública o presta un servicio público según la legislación nacional.¹¹⁶ En estos casos, la LCLDA señala la obligación de realizar una debida diligencia intensificada.

BENEFICIARIOS FINALES

El GAFI, en sus Recomendaciones 24 y 25, establece que los países deben garantizar la transparencia en la titularidad de las personas jurídicas para prevenir el uso indebido en actividades ilícitas como el LA/FT. Los países deben implementar medidas efectivas para identificar y verificar la identidad de los beneficiarios finales, asegurando que esta información sea precisa, actualizada y accesible para las autoridades. Estas medidas incluyen la implementación de mecanismos que aseguren que la información básica, incluyendo que la información suministrada al registro mercantil sea precisa y actualizada en tiempo oportuno.¹¹⁷

En la reciente EM, el GAFI señaló que el país presenta ciertas debilidades para garantizar que la información de BF sea precisa y actualizada. Es necesario que se empoderen mecanismos para obtener

¹¹³ Asamblea Legislativa. Ley contra el lavado de dinero y activos (1998), decreto 498. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0B869CC3-0E7E-44B0-AFB7-59AC74EA0849.pdf>

¹¹⁴ ídem.

¹¹⁵ Asamblea Legislativa. (1983) Constitución de la República de El Salvador., <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/69A06B07-4F30-4F0E-8FB1-D664A3E6D8CC.pdf>

¹¹⁶ Naciones Unidas. (2004). Convención de las Naciones Unidas contra la Corrupción. https://www.unodc.org/pdf/corruption/publications_unodc_convention-s.pdf

¹¹⁷ CFATF-GAFIC.(s.f.).Recomendación 24: unidades de inteligencia financiera. (<https://www.cfatf-gafic.org/index.php/es/documentos/gafi40-recomendaciones/435-fatf-recomendacion-29-unidades-de-inteligencia-financiera>)

información adecuada, precisa y actualizada sobre el BF y el control de las sociedades mercantiles y otras personas jurídicas.¹¹⁸ De igual manera, implementar medidas que identifiquen y describan los diferentes tipos, formas y características básicas de las personas jurídicas, así como los procesos para su creación y la obtención y registro de información básica sobre los BF. También se señaló una falta de análisis de las vulnerabilidades que pueden presentar otros tipos societarios, distintos a las sociedades anónimas, y las potenciales modalidades de abuso existentes, incluido el FT.¹¹⁹

Actualmente, la LCLDA al igual que el APL imponen a los SO la responsabilidad de identificar y verificar a los BF de las personas jurídicas con las que operan, asegurando que los datos sobre BF sean reales, precisos y accesibles. Las Instituciones Financieras (IF) y los SO deben implementar políticas de debida diligencia que permitan identificar a los verdaderos propietarios de los activos y prevenir el uso de estructuras opacas para ocultar actividades ilícitas. Adicionalmente, el sector privado y la población deberían implementar medidas de debida diligencia para conocer quienes se encuentran detrás de las transacciones. El cumplimiento de estas normativas es esencial para fortalecer la transparencia y la integridad del sistema financiero salvadoreño.

SUJETOS OBLIGADOS (SO)

Incluir a actores de riesgo es clave en la regulación LA/FT, para garantizar que no existan brechas que puedan ser explotadas para actividades ilícitas. La EM del GAFI reveló que en El Salvador existen 60,000 SO; sin embargo, solo el 33% de ese universo se encuentra registrada ante la UIF, lo que evidencia el incumplimiento de algunas de las obligaciones más relevantes, entre ellas la emisión de ROS.¹²⁰ Por tanto, El Salvador debe tomar medidas para asegurar el cumplimiento eficaz de las obligaciones que señala el marco regulatorio antilavado.

En el APL de 2023 se incluyen como SO a sectores emergentes, como los PSAD y PSB. Sin embargo, no se abordan algunos que pueden representar un alto riesgo de LA/FT, como los partidos políticos, el sector turismo, los fideicomisos, las droguerías, las asociaciones o fundaciones sin fines de lucro (AS-FL). En enero de 2024, el presidente de la Asamblea Legislativa expresó que las constructoras, droguerías, farmacéuticas, partidos políticos, organizaciones no gubernamentales y gremiales, serían incluidas en el anteproyecto.¹²¹ Hasta la fecha del presente informe no se conocen avances en las discusiones ni la inclusión formal de estos SO.

¹¹⁸ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (Ct. 286, p. 280). Informe de Evaluación Mutua de la República de El Salvador – GAFILAT

¹¹⁹ GAFILAT. (2024). (Ct. 286.p.280)

¹²⁰ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (pág 150, p549). Informe de Evaluación Mutua de la República de El Salvador – GAFILAT

¹²¹ Guzman, Jessica. El Mundo. (2024). Diputados modificarán dictamen aprobado de la nueva Ley contra el Lavado: incluirán a constructoras, farmacéuticas, partidos y oenegés. <https://diario.elmundo.sv/politica/diputados-modificaran-dictamen-aprobado-de-la-nueva-ley-contra-el-lavado-incluyan-a-constructoras-farmaceticas-partidos-y-oeneges>

PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES (PSAV):

Los Proveedores de Servicios Virtuales (PSAV) refieren principalmente a la infraestructura a través de la cual se realizan las actividades relacionadas con la tecnología de registro distribuido (TRD), como a través de la Blockchain de Bitcoin, la Blockchain the Ethereum u otras como Tron, Polygon o Avalanche. En las PSAV se pueden realizar transacciones de un usuario a otro dentro del mismo PSAV o fuera de, para realizar transferencias, compras, pagos, intercambios o programar contratos inteligentes.

En El Salvador los PSAV se refieren a personas jurídicas o naturales que realizan algunas de las actividades reguladas por la LEAD con el fin de prestar sus servicios y ofrecer productos dentro del territorio salvadoreño a través de sus plataformas o infraestructuras, estos pueden encontrarse domiciliados en El Salvador o pueden ser no domiciliados que promueven la comercialización de activos digitales¹²². Los PSAV para operar deben encontrarse registrados ante la CNAD o el BCR. En los Registros a cargo de la CNAD¹²³ y el BCR¹²⁴, se encuentran algunos de los PSAV registrados Bitfinex, Binance, Ditobanx, Blink y Chivo Wallet.

(i) Aplicación de estándares ALA/CFT.

La Recomendación 15 de GAFI, sobre el uso de nuevas tecnologías, subraya la importancia que los países y las instituciones financieras identifiquen los riesgos asociados con el uso de AV mediante nuevas tecnologías. En 2018, el GAFI¹²⁵ emitió una nota interpretativa de esta recomendación, especificando el uso de tecnologías de la información y de telecomunicaciones (TIC). Esta nota establece que, para el monitoreo y supervisión de los AV y los PSAV, se deben considerar algunos aspectos claves y aplicar las recomendaciones existentes, incluyendo la implementación de controles para la identificación y mitigación de riesgos relacionados con el LA/FT.

¹²² Decreto 643. Ley de Emisión de Activos Digitales. Fecha de publicación: 24 de enero de 2023. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0CDA225C-1B6C-4098-AC3A-D608933C643B.pdf>

¹²³ Registro de Proveedores de Servicios de Activos Digitales, CNAD <https://cnad.gob.sv/es/como-registrarse/psad/>

¹²⁴ Registro de Proveedores de Servicios Bitcoin, BCR <https://registro-bitcoin.bcr.gob.sv/web/proveedores-registrados>

¹²⁵ Financial Action Task Force. (2019). Public Statement, Mitigating risks from virtual assets, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Regulation-virtual-assets-interpretive-note.html>; Outcomes FATF Plenary, 20-22 February 2019 <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Outcomes-plenary-february-2019.htm>.

Gráfico 4

ASPECTOS A DESTACAR DE LA NOTA INTERPRETATIVA DE LA RECOMENDACIÓN 15 DE GAFI (2018) FECHA DE ADOPCIÓN (2019)



Fuente: Global Financial Integrity

La implementación de la Recomendación 15 refuerza la necesidad de supervisar de manera rigurosa a los PSAV, asegurando que operen dentro de un marco regulatorio que mitigue los riesgos asociados con el uso de AV. El monitoreo continuo y la adaptación de medidas preventivas a las nuevas tecnologías son esenciales para proteger el sistema financiero de amenazas emergentes. Esto posiciona a El Salvador en línea con los estándares internacionales, fortaleciendo su capacidad para prevenir el LA/FT en un entorno digital en constante evolución.

La nota interpretativa de 2018 destacó varios aspectos clave, incluida la clasificación de los AV como transmisores de valor. Estableció que las plataformas donde se realizan actividades con AV deben obtener una licencia y estar registradas, bajo la supervisión y monitoreo de autoridades competentes. Estas autoridades son responsables de regular adecuadamente para prevenir LA/FT, así como imponer sanciones cuando corresponda. La nota también enfatizó cinco recomendaciones importantes:

R.1: Mitigación de riesgos ALA/FT/PDAM, **R.10:** Debida diligencia del cliente para transacciones superiores a 1,000 USD/Euros, **R.16:** Disponibilidad de información sobre el emisor y beneficiario, **R.35:** Responsabilidad administrativa, civil y penal para los PSAV, incluyendo directores y gerentes; **R.37-40:** Cooperación internacional.

En materia de AV, el GAFI ha emitido varios documentos importantes relacionados con la Recomendación 15 y la implementación de nuevas tecnologías. El presente gráfico muestra una línea de tiempo de dichos documentos.



Fuente: Global Financial Integrity

En el 2023, el GAFI actualizó los estándares aplicables a los AV, y GAFILAT publicó una guía sobre tipologías de LA/FT en la región, que incluye casos de fraude, trata de personas y el narcotráfico en países como Guatemala, Colombia, Argentina y El Salvador. En esta guía, se destacó un caso de estafa en El Salvador relacionado con el uso de AV, el cual puede ilustrar ciertos comportamientos en el propio país sobre este tema.¹²⁶ En la actualización de la Recomendación 15, el GAFI, se enfocó en tres aspectos: la falta de

¹²⁶ GAFILAT. (2023). Informe de Tipologías Regionales de LA/FT 2021-2022. <https://biblioteca.gafilat.org/wp-content/uploads/2024/07/Informe-de-Tipologias-Regionales-de-LA-2021-2022.pdf>

estudios de riesgo sólidos en jurisdicciones que ya han regulado AV, los desafíos en la implementación de la regla del viajero, y la necesidad de una prevención efectiva mediante el envío de ROS (Recomendación 20).

El APL incorpora a los PSAV y PSAD, como SO, lo cual no está contemplado en la LCLDA vigente. Este cambio se produce tras la aprobación de la Ley Bitcoin 2021 y la aprobación de la LEAD en 2023, así como en respuesta a las directrices de GAFI/GAFILAT para mitigar riesgos ALA/FT para los países miembros.

Desde una perspectiva de desafíos y oportunidades, la inclusión de los PSAV como SO en el APL representa un avance significativo para El Salvador en la adaptación a las mejores prácticas internacionales en la supervisión de AV. Sin embargo, la implementación de estos estándares presenta la necesidad de establecer marcos regulatorios sólidos y realizar evaluaciones de riesgos continuas. La función de supervisión y sanción por parte de las autoridades ante el incumplimiento de la normativa ALA/FT requerirá de la coordinación interinstitucional, la cooperación internacional y la cooperación del sector privado.

(ii) Evaluación de Riesgo (ER) y Enfoque en Políticas Aplicables a los PSAV

El GAFI publicó un reporte sobre el estatus de la implementación de la Recomendación 15 en miembros del GAFI y jurisdicciones adicionales, donde identificó que el 2.9% de las jurisdicciones analizadas no han realizado una evaluación de riesgo en relación con los AV. Además, el 4.64% no poseen regulación sobre AV que mitigan los riesgos ALA/CFT

adecuados¹²⁷. El GAFI establece¹²⁸ que las jurisdicciones que aún no han identificado los riesgos asociados con el LA/FT en el uso de AV y PSAV deben hacerlo para implementar medidas de mitigación apropiadas. Asimismo, recomienda que las jurisdicciones supervisen y monitoreen a los PSAV, independientemente si permiten o prohíben el uso de AV, aplicando sanciones en caso de incumplimiento de los estándares ALA/CFT, subraya la importancia de una regulación y supervisión efectivas.

El Salvador, realizó una ENR recientemente, donde los resultados de la EM sobre esta recomendación establecen que "No existe una evaluación de riesgos de LA/FT para los PSAV ni faculta a la entidad supervisora para un monitoreo basado en riesgo".¹²⁹ A pesar de que desde 2021¹³⁰ El Salvador ha aprobado más de 20 regulaciones relacionadas a los AV, es necesario que formen parte de una política pública suficientemente amplia e integral que promueva la tecnología, la inclusión financiera y la protección de datos.

Para construir un ecosistema sólido de AV, es fundamental implementar campañas de alfabetización financiera y tecnológica, fomentar el diálogo

¹²⁷ Financial Action Task Force. (2024). "Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity", <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf.coredownload.pdf>

¹²⁸ Financial Action Task Force. (2024). Virtual assets: targeted update on implementation of the FATF Standards on VAs and VASPs. Pág. 4 <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html>

¹²⁹ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador.(Ct188- pág 259). Informe de Evaluación Mutua de la República de El Salvador – GAFILAT

¹³⁰ Cripto Abierto. (s.f). Regulación Cripto.<https://criptoabierto.com/regulacion-cripto/>

entre los diferentes sectores, incluido al sector privado tradicional, y capacitar a las fuerzas del orden en el uso y la regulación de estas tecnologías.¹³¹ Adicionalmente, es crucial fortalecer a los entes reguladores, supervisores y a cargo de las sanciones.

OBLIGACIONES DE REPORTE DE OPERACIONES SOSPECHOSAS PARA PSB Y PSAD

En la actualidad los PSAV no son sujetos obligados, por lo tanto, el APL exige que los sujetos obligados alerten sobre ROS en caso de identificar banderas rojas en las transacciones de AV, facultando a la UIF para implementar actividades de prevención del delito y sensibilización en la materia, así como para crear e implementar instructivos dirigidos a los PSB/PSAD, con el fin de asegurar su cumplimiento. Sobre la Recomendación 20 de los ROS aplicable a los AV, el GAFI emitió un informe sobre tipologías que abordan la anonimidad, el origen de los fondos y patrimonio, las transacciones, los riesgos geográficos y las características de los remitentes y destinatarios¹³².

Por otro lado, la Oficina para el Control de Activos Extranjeros del Dep. de Tesorería de Estados Unidos (OFAC) ha publicado la lista Nacional Especialmente Designada (SDNL-Specially Designated National List en inglés), que incluye direcciones de AV

sancionados. Estas direcciones fueron removidas con una resolución de apelación reciente. Es indispensable que los proveedores monitoreen constantemente estas listas para asegurar el cumplimiento de las regulaciones y evitar involucrarse en transacciones ilícitas.

En cuanto a este aspecto, los resultados de la EM del GAFILAT establecen que, con la aplicación de software de trazabilidad de transacciones con AV y Bitcoin, los supervisados tienen claridad sobre las direcciones sancionadas y los listados correspondientes.¹³³ La evaluación también destacan la obligación del supervisor de emitir directrices o información que ayude a los PSAD, certificadores, emisores y adquirentes (o inversionistas) a aplicar las medidas nacionales ALA/CFT y en particular, a detectar y reportar las operaciones sospechosas¹³⁴ dentro del proceso de emisión de AV, lo cual se explicará más adelante en la sección de tokenización.

La implementación efectiva de los ROS es crucial para detectar y mitigar riesgos asociados con el uso de AV. El monitoreo constante y la capacidad de los PSB/PSAD para identificar transacciones sospechosas garantizan que el sistema financiero se mantenga resiliente ante las amenazas emergentes. La UIF y los entes supervisores desempeñan un papel fundamental al proporcionar las herramientas y la orientación necesarias para que los SO puedan identificar y reportar estas transacciones de manera oportuna y efectiva.

¹³¹ Global Financial Integrity and Vance Center. (2023). The Virtual Assets Ecosystem In El Salvador: Strengthening Financial Integrity And Transparency. <https://34n8bd.p3cdn1.secureserver.net/wp-content/uploads/2023/10/Crypto-El-Salvador-Report-ENG-FINAL-1.pdf?time=1724969507>

¹³² Si una institución financiera sospecha o tiene motivos razonables para sospechar que los fondos son producto de una actividad criminal, o están relacionados al financiamiento del terrorismo, a ésta se le debe exigir, por ley, que reporte con prontitud sus sospechas a la Unidad de Inteligencia Financiera (UIF). <https://biblioteca.gafilat.org/wp-content/uploads/2024/07/Recomendaciones-metodologia-act-DIC2023.pdf>

¹³³ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. Página 114. Informe de Evaluación Mutua de la República de El Salvador – GAFILAT.

¹³⁴ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (CT178, pág. 257).

BENEFICIARIOS FINALES (BF) Y PSB/PSAD

Hemos comentado sobre la importancia de conocer a los BF y de seguir las recomendaciones internacionales al respecto. El Salvador no cuenta, dentro de su marco regulatorio, con una definición robusta de BF ni tampoco con un registro específico para ellos. Por el contrario, el APL exige que cada SO, en este caso los PSB/PSAD, identifiquen a los BF de cada empresa, con el objetivo de reconocer la persona natural atrás de la persona jurídica.

LA REGLA DEL VIAJERO

La aplicación de la regla del viajero promueve la transparencia bajo la Recomendación 16 de GAFI en el contexto de AV. El GAFI ha identificado varios retos en su implementación, especialmente relacionados con la recolección de información y la interoperabilidad entre herramientas que recopilan datos.

Sobre la regla del viajero, los resultados de la EM destacan los siguientes aspectos:

i) Los PSAD y PSB no escanean la información requerida del originante sobre las transferencias de AV, ni se especifica la información de origen de una transacción de AV o Bitcoin. Es decir, no solo debería identificarse al originante a través de un debido proceso de KYC, sino también al destinatario, mediante la plataforma en la que se tenga una cuenta de usuario. Esto aplicaría tanto a personas naturales como jurídicas, implicando un debido proceso de KYB. Además, GAFILAT establece que la información de transacción deberá estar debidamente identificada, a lo que se conoce como KYT.

ii) No se advierte que El Salvador determina las mismas obligaciones a las instituciones financieras sobre el origen o el envío de transacciones. En este sentido, resulta crucial la participación y coordinación entre el sector financiero tradicional y el sector de los AD, incluyendo PSAD y PSB. Un ejemplo relevante de la implementación de la regla del viajero en su relación entre una institución financiera y los PSAD, es Europa que ha aplicado su regulación sobre criptoactivos.¹³⁵

El Salvador, dentro de su marco normativo de mejora regulatoria, tiene la facultad legal para realizar estudios de impacto regulatorio (EIR)¹³⁶, lo que sería de gran valor para la implementación de regulaciones en tecnología y finanzas, eliminando barreras burocráticas y cumpliendo con la supervisión del sector.¹³⁷ Que El Salvador implemente efectivamente la regla del viajero, es crucial involucrar al sector financiero y a los PSAD y PSB, para considerar las particularidades financieras y tecnológicas del país. En la reforma a la LEAD se especifica que no se aplicará la Ley de Mejora Regulatoria por parte de la CNAD¹³⁸; sin embargo, se tendrá en cuenta la aplicación de los principios de mejora regulatoria para estos efectos.

¹³⁵ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (CT 180, pág. 257, 258).

¹³⁶ Una evaluación de impacto regulatorio es un “proceso de análisis sistemático de los objetivos, opciones e impactos de las regulaciones, a fin de garantizar que sus beneficios sean superiores a sus costos en la sociedad y que dichas regulaciones representan la mejor alternativa para atender una problemática específica”. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/2A937770-6A46-4FDD-B890-FEBAF034B0DA.pdf>

¹³⁷ Asamblea Legislativa. (2019). Ley de Mejora Regulatoria. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/3EA48492-AC1C-4CDD-BD2E-5AA2B8CEADB0.pdf>

¹³⁸ Asamblea Legislativa (2024). Reformas a la Ley de Emisión de Activos Digitales. Arts. 42-A y 42-B, <https://x.com/asambleasv/status/1841985362903683367?s=48>

DEBIDA DILIGENCIA DEL CLIENTE Y PSAV

En materia de prevención de LA/FT, la DDC es crucial para recolectar información que impida la entrada de actores ilícitos al sistema. Sin embargo, la información almacenada por los PSAV puede ser compartida para investigar y perseguir delitos, permitiendo identificar al titular de la cuenta y rastrear sus transacciones. La implementación de la DDC es esencial para proteger la integridad del sistema financiero, pero también es importante garantizar que la información recopilada se maneje con la máxima confidencialidad y seguridad.

El APL establece el uso de procesos como la autenticación, registros biométricos, escaneos de tarjetas de identificación, localización y reconocimiento de Internet Protocol (IP). También se requiere que los PSAD y PSB tengan la capacidad para rastrear las transacciones. Conforme a la Recomendación 10 del GAFI, la DDC permite evitar interactuar con actores sancionados, lo cual puede lograrse mediante la implementación de la regla del viajero.

COOPERACIÓN INTERNACIONAL: INVESTIGACIÓN DE CUENTAS DE PSAD, CONGELACIÓN/INCAUTACIÓN Y RECUPERACIÓN DE ACTIVOS

Los resultados de la EM señalan que “No existe una sanción apropiada hacia los PSB y PSAD, incluyendo directores y directivos”.¹³⁹ Dentro de la legislación salvadoreña, la CNAD y la SSF tienen la facultad

legal de sancionar a los PSAD y PSB que no cumplan con los estándares ALA/CFT. Los resultados de la EM destacan que los PSB poseen herramientas tecnológicas que permiten el congelamiento de AD,¹⁴⁰ lo cual es un hallazgo importante para el país y una referencia para el tema de congelamiento de AD. Otras jurisdicciones, como el Reino Unido, han optado por regular directamente estos procedimientos,¹⁴¹ estableciendo procesos.

Es crucial que las autoridades apliquen disposiciones sobre la cadena de custodia de la evidencia digital para su autenticación en procesos judiciales.¹⁴² La cooperación con el sector privado es esencial para obtener información sobre cuentas investigadas, como datos personales al momento de la creación de la cuenta, dirección de la billetera, estado de cuenta y dirección IP.

La cooperación internacional y la preservación de evidencia digital son fundamentales para la efectividad de la lucha contra el LA/FT. En los resultados de la EM para El Salvador, se destacan que en materia de cooperación internacional existen dudas respecto de los PSAV pueden proporcionar rápida,

¹³⁹ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (pág. 319). Informe de Evaluación Mutua de la República de El Salvador – GAFILAT

¹⁴⁰ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (p.6 literal g). Informe de Evaluación Mutua de la República de El Salvador – GAFILAT “El país cuenta con un sistema que le permite implementar SFD con base en las RCSNU relevantes, el cual ha sido reformado en enero de 2024 para procurar que los congelamientos sean aplicados sin demora. En esta línea, las instituciones financieras y proveedores de servicios de bitcoin (PSB), monitorean las listas por medio de herramientas tecnológicas y están en posibilidad de inmovilizar bienes o detener operaciones en los casos en los que se detectan coincidencias”.

¹⁴¹ Stolen Asset Recovery Initiative. (2022). Guid United Kingdom-update 2022, Stolen Asset Recovery Initiative, <https://star.worldbank.org/publications/asset-recovery-guide-united-kingdom-update-2022>

¹⁴² Chainalysis. (2024). The 2024 State of cryptocurrency investigations report. <https://go.chainalysis.com/state-of-crypto-investigations-report-2024.html>

constructiva y eficazmente la mayor gama posible de cooperación internacional en esta materia.¹⁴³

¹⁴³ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (pág. 319). Informe de Evaluación Mutua de la República de El Salvador – GAFILAT.

2

CAPÍTULO 2

Riesgos del Ecosistema de AV y Delitos Financieros



Esta sección del informe identifica los riesgos en el ecosistema de AV en El Salvador y propone medidas para combatirlos.

AV Y RIESGOS DE DELITOS FINANCIEROS EN EL SALVADOR

En nuestro informe anterior, se determinaron varios delitos subyacentes de LA/FT en el país, como tráfico de personas, extorsión, mercancía de contrabando, narcotráfico y peculado.¹⁴⁴ Un caso concreto es una estafa agravada que involucró a inversionistas del mercado de criptomonedas de EE.UU., generando al estafador entre el 25% y 65% de ganancias mensuales.¹⁴⁵ Tanto personas jurídicas como naturales fueron estafadas por montos superiores a US\$10,000.¹⁴⁶

Los delitos contemplados en la Ley Especial Contra Delitos Informáticos y Conexos (LECDIC) relacionados con la afectación de sistemas tecnológicos de información, como la supuesta difusión del código fuente de uno de los cajeros Chivo ubicado en la ciudad de San Miguel¹⁴⁷. Esta información fue publicada en un sitio web que fue confiscado por el

FBI en mayo de 2024.¹⁴⁸ Chivo, S.A. de C.V. aseguró, a través de su cuenta dentro de la plataforma X el 23 de abril de 2024, que los datos de los usuarios estaban protegidos y que la información sustraída solo correspondía a la operatividad del cajero¹⁴⁹.

La FGR también publicó en sus redes sociales sobre otros casos relacionados al uso de AV, como la captura de individuos por el delito de agrupaciones ilícitas, en donde se incautaron bienes tangibles, incluyendo dispositivos electrónicos y criptomonedas, con un valor que asciende a más de US\$50,000.¹⁵⁰ Así como, la incautación de billeteras frías de criptomonedas por estar relacionadas en actividades de piratería digital,¹⁵¹ bajo la jurisdicción salvadoreña.

A pesar de la existencia de una política de ciberseguridad¹⁵² que protege la infraestructura crítica de las instituciones públicas en El Salvador, medios de comunicación han informado sobre la publicación de credenciales de ciudadanos, lo que representa una brecha de seguridad sumamente grave.

¹⁴⁴ Global Financial Integrity and Vance Center. (2023). The Virtual Assets Ecosystem In El Salvador: Strengthening Financial Integrity And Transparency. <https://34n8bd.p3cdn1.secureserver.net/wp-content/uploads/2023/10/Crypto-El-Salvador-Report-ENG-FINAL-1.pdf?time=1724969507>

¹⁴⁵ Fiscalía General de la República. [@FGR_SV] (2024). #Captura. La @FGR ordenó la captura de M., por esta agravada. [post X] https://x.com/FGR_SV/status/1813584006312591409

¹⁴⁶ Fiscalía General de la República. [@FGR_SV] (2024).

¹⁴⁷ Chivo Wallet. [@chivowalltet] (2024). Comunicado de prensa. Los datos de nuestros usuarios están protegidos y en ningún momento se ha violado la seguridad de chivo.[post X]. <https://x.com/chivowallet/status/1782992751354655118?s=46>

¹⁴⁸ Breach Forums. (s.f.) Raidforums Reporting Form. Federal Bureau of Investigation (FBI). <https://breachforums.ic3.gov/>

¹⁴⁹ Chivo Wallet. [@chivowalltet] (2024). Comunicado de prensa. Los datos de nuestros usuarios están protegidos y en ningún momento se ha violado la seguridad de chivo.[post X]. <https://x.com/chivowallet/status/1782992751354655118?s=46>

¹⁵⁰ Fiscalía General de la República. [@FGR_SV] (2024). #Allanamiento. En la vivienda se incautaron de una laptop, una tablet, una lujosa camioneta, 6 teléfonos celulares y más de US\$50,000 en criptomonedas. [post X2]. https://x.com/fgr_sv/status/1545831698797137922?s=48

¹⁵¹ Fiscalía General de la República. [@FGR_SV] (2024). #Condena. La @FGR logró que cada uno de los 8 imputados acusados de piratería digital, fueran condenados a 3 años de prisión. https://x.com/fgr_sv/status/1808293547289813021?s=48

¹⁵² Diario Oficial de El Salvador. (2022) Política de Ciberseguridad El Salvador (No.90 Tomo. 435)

Esto podría permitir que ciberdelincuentes utilicen la información obtenida para realizar ciberataques, falsificación de credenciales o fraudes informáticos dentro del sistema financiero tradicional y los PSAD/PSB.

Por otra parte, una falta de aplicación efectiva de estándares para prevenir LA/FT en los beneficiarios finales y programas de ALA/CFT podría promover la opacidad en las inversiones en Bitcoin y AD. Es importante destacar que algunos PSAD han colaborado con la FGR de El Salvador, fortaleciendo la cooperación entre el sector privado.¹⁵³

Los riesgos emergentes para el ecosistema de AV en El Salvador incluyen la posibilidad de ataques cibernéticos, el uso indebido de criptomonedas para los flujos financieros ilícitos, la falta de transparencia en las inversiones y los riesgos para el LA/FT. A continuación, se exponen algunos de los riesgos emergentes para el ecosistema de AV en El Salvador:

CIUDADANÍA POR INVERSIÓN (CBI)

En diciembre de 2023, El Salvador aprobó una ley que establece un camino hacia la ciudadanía salvadoreña para los inversionistas que donen Bitcoin a programas gubernamentales específicos¹⁵⁴. La ley permite a los inversionistas omitir el período

de residencia permanente de 5 años antes de solicitar la ciudadanía.¹⁵⁵ El programa está limitado a 1,000 inversionistas anualmente, cada uno contribuyendo con US\$1 millón. Los resultados de la EM señalan que existen dudas sobre si se implementan los estándares de DDC para los aplicantes, y si se mitigan los posibles riesgos LA/FT.¹⁵⁶

TOKENIZACIÓN DE ACTIVOS DEL MUNDO REAL

La clasificación de los tokens de activos como valores requiere cumplir con regulaciones que aseguren transparencia y protección al inversor¹⁵⁷. Esto incluye procedimientos de cumplimiento ALA/CFT y KYC, fundamentales para garantizar la integridad y seguridad de las transacciones. Además, se deben implementar medidas de protección al consumidor, medidas de seguridad de la información y gestión de riesgos, alineadas con los estándares del GAFI para prevenir actividades delictivas. Los resultados de la EM identificaron que aún existen debilidades en la identificación y evaluación de riesgos de LA/FT en los PSAD,¹⁵⁸ incluyendo aquellos involucrados en la emisión de AD.

¹⁵³ Binance (2024). Binance extiende su colaboración en materia de seguridad junto a la FGR de El Salvador. https://www.binance.com/es-LA/blog/markets/binance-sigue-ampliando-su-colaboracion-en-materia-de-seguridad-junto-a-la-fiscal-general-de-la-rep%C3%ABlica-de-el-salvador-14-58883079379785511?utm_medium=navigator_share_link

¹⁵⁴ Asamblea Legislativa. (2023). Decreto 918. Reforma a ley especial de migración y extranjería. <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/86F735AF-0AEE-4330-8509-04C9938296D2.pdf>

¹⁵⁵ Arbaiza, Gerardo. (2023). Reuters. El Salvador Offers Citizenship to Foreign Bitcoin Investors, U.S. [https://www.usnews.com/news/world/articles/2023-12-21/el-salvador-offers-citizenship-to-foreign-bitcoin-investors#:~:text=SAN%20SALVADOR%20\(Reuters\)%20%2D%20El,social%20and%20economic%20development%20programs](https://www.usnews.com/news/world/articles/2023-12-21/el-salvador-offers-citizenship-to-foreign-bitcoin-investors#:~:text=SAN%20SALVADOR%20(Reuters)%20%2D%20El,social%20and%20economic%20development%20programs)

¹⁵⁶ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (p.24 pág. 21). Informe de Evaluación Mutua de la República de El Salvador – GAFILAT.

¹⁵⁷ Bimount, "Tokenización de Activos- Part II: Regulaciones y Riesgos" (2023). <https://bimount.io/tokenizacion-de-activos-regulaciones-y-riesgos/>

¹⁵⁸ GAFILAT. (2024). Informe de evaluación mutua de la República de El Salvador. (CT 188, P. 259). Informe de Evaluación Mutua de la República de El Salvador – GAFILAT.

Como parte de la tokenización, se han identificado riesgos para la infraestructura como ingeniería social para ganar acceso no autorizado a las plataformas de intercambio, explotación del token a través de la manipulación de la data ingresando a la Blockchain¹⁵⁹, o ataques a liquidity pools¹⁶⁰, es decir a los tokens contenidos dentro de los contratos inteligentes. Por ello, los estándares de seguridad de la información son esenciales de aplicación para los proveedores de servicios digitales, con el fin de prevenir y mitigar los riesgos correspondientes. En el presente informe se presentan dos estudios de caso de tokenización a manera de ejemplo de cómo se abordan en El Salvador: Tokenización de productos agrícolas, bienes raíces y tokenización de deudas y fondos. Los casos incluyen la legislación pertinente, los beneficios, y los procesos a considerar en cada caso.

TOKENIZACIÓN DE PRODUCTOS AGRÍCOLAS

En abril de 2024, la CNAD autorizó la tokenización de productos agrícolas,¹⁶¹ la cual consistió en la emisión de un token cuyo AD subyacente era un bushel de soja, equivalente a aproximadamente sesenta libras de soja. Los tokens se ofrecieron en una plataforma digital gestionada por un PSAD registrado en la CNAD, así como el Documento de Información Relevante (DIR), certificado y presen-

tado a la institución para la autorización de la emisión de los AD. Los tokens circularon en las redes de Blockchain de Polygon,¹⁶² Avalanche¹⁶³ y Linea¹⁶⁴ Blockchains, con un total de 7,600,000 tokens, residiendo en la cadena de bloques de Ethereum.

En cuanto a la fiscalidad, el DIR establece que los impuestos variarán según la jurisdicción nacional del adquirente. En el caso de El Salvador seguirán las reglas del artículo 36 de la LEAD, que otorga exenciones fiscales sobre el valor nominal del AD o sus rendimientos. Esta exención también se aplica al emisor del registro, al certificador y al PSAD dentro de la CNAD, incluyendo las ganancias o beneficios de los stakeholders y socios de las personas jurídicas registradas.

¹⁵⁹ Benz, Mike, "Risks associated with decentralized finance exploitation, Top 10 vulnerabilities you need to know", 2023. Medium. <https://medium.com/@realMikeBenz/risks-associated-with-decentralized-finance-exploitation-top-10-vulnerabilities-you-need-to-know-848f923964c5>

¹⁶⁰ Antolin, Mike, "What are liquidity pools?", Coindesk, 2022. <https://www.coindesk.com/learn/what-are-liquidity-pools/>

¹⁶¹ Egrains. (2024). Notificación de inicio de oferta pública. <https://cnad.gob.sv/wp-content/uploads/2024/06/20240117-egrains-anuncio-de-oferta-publica.pdf>

¹⁶² Polygonscan.(s.f.).The address of the smart contract were the tokens were issued is: 0xb9AE6304706e78d1bb28daCc645499bcF55D6852 <https://polygonscan.com/address/0xb9ae6304706e78d1bb28dac-c645499bcf55d6852>

¹⁶³ Snowtrace. (s.f.).The address of the smart contract were the tokens were issued is: 0xb9AE6304706e78d1bb28daCc645499bcF55D6852 <https://snowtrace.io/address/0xb9AE6304706e78d1bb28daCc645499bcf55d6852>

¹⁶⁴ Linea. (s.f.) The address of the smart contract were the tokens were issued is: 0xb9AE6304706e78d1bb28daCc645499bcF55D6852 <https://lineascan.build/address/0xb9ae6304706e78d1bb28dac-c645499bcf55d6852>

Gráfico 6

ESTUDIO DE CASO: TOKENIZACIÓN DE ACTIVOS DEL MUNDO REAL PARA COMMODITIES



Fuente: GFI con información del Documento de Información Relevante de la Emisión del token \$ESoy disponible en la página de eGrains

TOKENIZACIÓN DE DEUDAS Y FONDOS

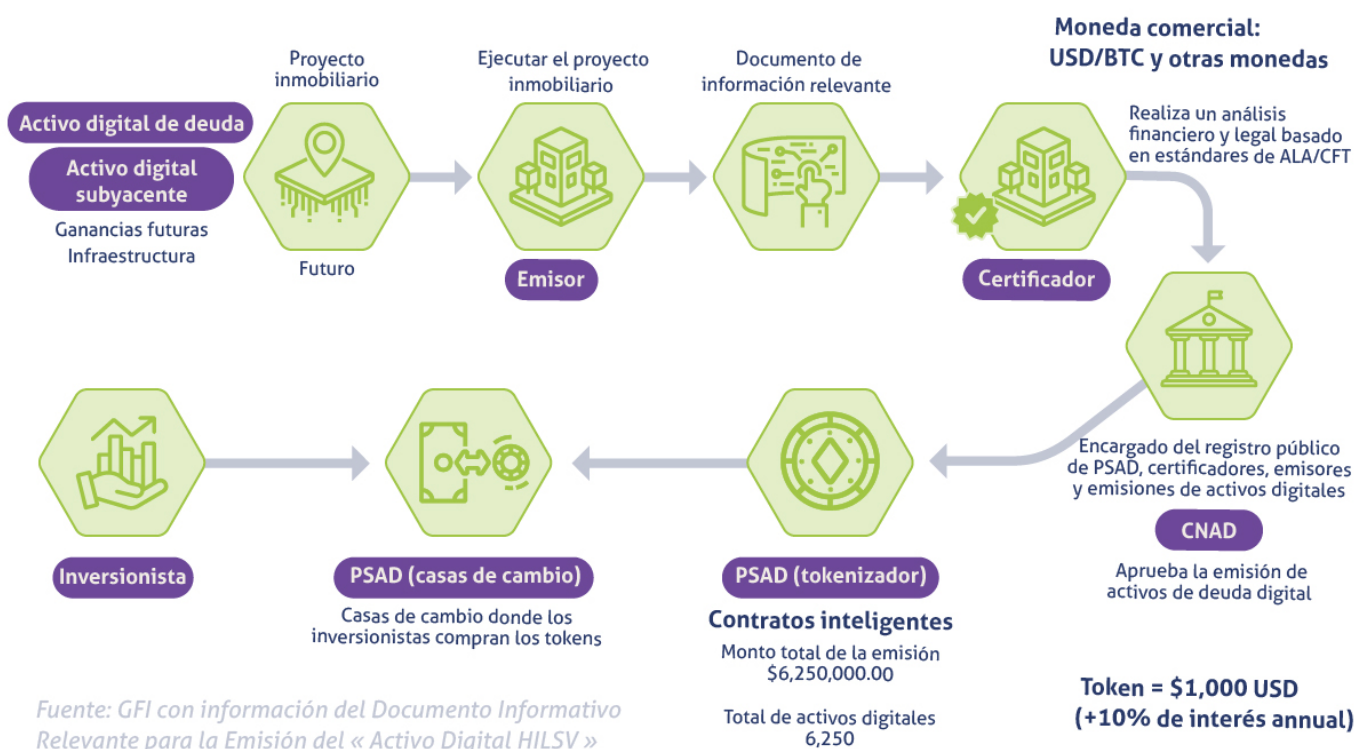
Al igual que en el proceso de emisión de AD anterior, intervienen: el emisor, el certificador, el tokenizador y, finalmente, la plataforma de intercambio o el PSAD. Todos deben estar registrados ante la CNAD. Para este tipo de emisión, es necesario consignar en el DIR toda la información técnica, financiera y legal, para proporcionar transparencia a los posibles inversionistas.

En el ejemplo a continuación, el AD es una deuda, el activo subyacente es el flujo futuro de efectivo y la infraestructura del proyecto es construcción. La CNAD autoriza la emisión de estos AD de deuda en una oferta pública. Posteriormente, el tokenizador o PSAD a cargo de la creación de los contratos inteligentes que contienen los tokens puede proceder tecnológicamente a emitirlos dentro de la cadena de bloques. Una vez emitidos, los tokens pueden ser intercambiados dentro de la plataforma del PSAD, que facilita el contacto con los inversionistas. Toda la información relacionada con la emisión debe publicarse en las páginas web de la plataforma del PSAD, del tokenizador y también del emisor¹⁶⁵.

¹⁶⁵ Asamblea Legislativa. Ley de Emisión de Activos Digitales. (2023). <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/OCDA225C-1B6C-4098-AC3A-D608933C643B.pdf>

Gráfico 7

ESTUDIO DE CASO: TOKENIZACIÓN DE ACTIVOS DE DEUDA EN EL MUNDO REAL



LA EMISIÓN DE STABLECOINS

Las monedas estables son “un tipo de activo digital diseñado para tener un valor estable, que hace referencia, representa o está respaldado por una o varias monedas fiduciarias u otro activo subyacente que mantiene baja volatilidad”.¹⁶⁶

En junio de 2024, la CNAD autorizó la emisión de la stablecoin aUSD₡. Esta emisión permitió a dos PSAD promover la stablecoin Alloy de Tether (AbT). Este token permitirá a los usuarios acuñar aUSD₡ utilizando Tether Gold (XAU₡) como activo colateral, lo que resultará en una moneda digital respaldada por el valor del oro. Como parte de las obligaciones de la LEAD, el DIR que cumplió con el proceso de certificación,¹⁶⁷ ha sido publicado en la página web de su promoción. Los tokens están disponibles en la cadena de bloques de

¹⁶⁶ Ministerio de Economía de El Salvador, Reformas a la Ley de Activos Digitales, 2024.

¹⁶⁷ TR. Capital. (2024). Stablecoin issuance public offering certification report https://alloy.tether.to/docs/stablecoin_issuance_public_offering_certification_report.pdf

Ethereum y no hay un número de tokens requerido o autorizado para su emisión; el DIR establece que el número de aUSD₮ dependerá del mecanismo de oferta y demanda.

El DIR también establece que solo los clientes que completen el proceso de incorporación KYC podrán interactuar con estos tokens¹⁶⁸. Además, se advierte sobre los riesgos asociados, como fluctuaciones de precios y riesgos de mercado, fiabilidad de la información de precios, riesgo de liquidación, inclusión en listas negras y bloqueo de direcciones, interrupción y accesibilidad de la plataforma, amenazas de ciberseguridad, insolvencia de otros usuarios, riesgos regulatorios, conflictos de interés, riesgos relacionados con terceros y el riesgo asociado con el activo colateral (Tether Gold). También se anima a los clientes a cumplir con el proceso de verificación antes de usar el servicio, y a cumplir con las normativas internacionales, como los estándares del GAFI, la Ley de Secreto Bancario de los Estados Unidos de América, y las regulaciones ALA/CFT de las Islas Vírgenes Británicas, y El Salvador¹⁶⁹.

El régimen fiscal aplicable en El Salvador exime a estos tokens de cualquier tipo de impuestos, tasas o contribuciones, ya sean ordinarias o extraordinarias, y otorga exenciones a las ganancias de capital o ingresos derivados de la compraventa o cualquier otro medio de transferencia, incluida la condonación de deudas, de estos tokens, según lo establece el DIR.

¹⁶⁸ Ídem.

¹⁶⁹ Ídem.

FINANCIAMIENTO POLÍTICO

Incorporar los AV al financiamiento político plantea ciertos desafíos en términos de transparencia y rendición de cuentas, debido a la pseudo anonimidad y descentralización inherente de los AV. Debido a que no hay una regulación específica sobre la materia, se ha generado debate sobre la conveniencia y potenciales riesgos asociados al uso de AV en el financiamiento de la política.

En El Salvador, los partidos políticos son sujetos obligados,¹⁷⁰ de acuerdo con la LCLDA. Por tanto, tienen obligaciones¹⁷¹ en materia de prevención y detección LA/FT. Entre estas obligaciones se incluyen: inscribirse en la UIF, nombrar un oficial de cumplimiento, mantener un programa ALA/FT con enfoque de riesgo, reportar operaciones sospechosas, establecer una política interna de debida diligencia para identificar donantes, y conservar la documentación de las operaciones por un periodo de cinco años. No obstante, a la fecha no se evidencian obligaciones específicas relacionadas con las donaciones a través del uso de AV, especialmente Bitcoin, que puede ser utilizado, según su ley, en cualquier transacción y a cualquier título que las personas naturales o jurídicas, públicas o privadas requieran realizar.

¹⁷⁰ Asamblea Legislativa. (1998). Ley Contra El Lavado de Dinero y Activos. <https://ssf.gob.sv/wp-content/uploads/2022/07/Ley-contra-el-lavado-de-dinero-y-de-Activos-D498.pdf>

¹⁷¹ Fiscalía General de la República. (2021). Instructivo de la unidad de investigación financiera para la prevención del lavado de dinero y de activos. <https://www.uif.gob.sv/wp-content/uploads/instructivos/InstructivoUifDiarioOficial2021.pdf>

Durante las elecciones de febrero y marzo de 2024, la mayoría de los partidos declararon no tener la intención de recibir donaciones a través de AV, aunque algunos señalaron estar estudiando el tema.¹⁷² Ello compromete al Tribunal Supremo Electoral (TSE), como responsable del monitoreo y control del financiamiento político, a establecer lineamientos sobre el funcionamiento, los riesgos y tipologías asociadas al uso del ecosistema digital, al igual que potencialmente una supervisión efectiva respecto a los ROS que se presenten a la UIF por parte de los partidos.

Respecto a los niveles de transparencia y aportes recibidos por los partidos políticos en El Salvador, es complejo considerar el involucramiento de los AV cuando provengan tanto de financiamiento público o privado, al igual que la debida diligencia de los propios partidos y el TSE para tener trazabilidad sobre los fondos, especialmente si no hay una normativa clara al respecto.

Este escenario muestra la necesidad de reforzar la regulación y supervisión del financiamiento político en general.

Un marco regulatorio sólido para la fiscalización y auditoría, acompañado de una entidad eficaz de supervisión, son necesarios para fiscalizar y monitorear las donaciones a través de cualquier tipo de monedas o especies. Sin embargo, es indispensable exigir el cumplimiento normativo a los SO y aplicar sanciones disuasorias, en caso de cumplimiento.

Tanto la regulación como su aplicación son imprescindibles para establecer un entorno de integridad en la política. De lo contrario, podría crearse un ambiente atractivo para el LA, la corrupción o el financiamiento ilícito a través de donaciones anónimas, extranjeras o que sobrepasen el umbral permitido.

La potencial adquisición de AV con dinero de procedencia ilícita y su posterior donación a partidos políticos, es uno de los riesgos que puede enfrentar el financiamiento político. El uso de plataformas de “mixing” o “tumbling” para criptomonedas puede constituir otra estrategia para borrar el rastro de las transacciones y ocultar la identidad del comprador de AV y posterior donante de un partido político.

Otro riesgo del uso de los AV en la política es la posibilidad de superar los umbrales permitidos por la Ley de Partidos Políticos (LPP). Aunque en El Salvador no existe un límite máximo para las donaciones privadas, se prohíbe superar individualmente el monto del dos por ciento del presupuesto del año anterior, aprobado por la Asamblea Legislativa al TSE.¹⁷³ Esta prohibición puede eludirse con el uso de AV, dividiendo los montos en cantidades menores por debajo del umbral y enviándolos desde múltiples direcciones. Un proceso adecuado de verificación y alerta por parte de los PSAD/PSB podría detectar esta práctica.

¹⁷² Accion Ciudadana. (2022). Informe de transparencia 2021: Análisis de los ingresos y gastos de los partidos. (p. 50). Informe de transparencia 2021: Análisis de los ingresos y gastos de los partidos políticos (accion-ciudadana.org)

¹⁷³ Asamblea Legislativa.(1993). Ley de partidos políticos. (art. 65). C212CE14-561E-401D-822F-A38E38483397.pdf (asamblea.gob.sv)

3

CAPÍTULO 3

PSAV en El Salvador y la Protección de Datos Marco Legal de Protección de Datos en El Salvador



El Salvador cuenta con regulaciones sobre protección de datos, como la Ley de Acceso a la Información Pública (LAIP)¹⁷⁴ y la LECDIC.¹⁷⁵ Sin embargo, no existe una normativa específica para la protección de datos personales hasta la fecha de este informe, ya que el proyecto de Ley de Protección de Datos (LPD) fue vetado por el Presidente de la República en mayo de 2021.¹⁷⁶ Por otro lado, en marzo de 2022, se aprobó el Acuerdo 163 que contiene la Política de Ciberseguridad, cuyo objetivo principal es la prevención de riesgos cibernéticos¹⁷⁷ y la protección de datos informáticos de la infraestructura crítica del Estado.

En este capítulo haremos referencia a legislación internacionales a manera de referencia, billeteras digitales y el caso concreto de Chivo Wallet para el caso de El Salvador.

A. REFERENCIA INTERNACIONAL

(i) Reglamento General de Protección de Datos (RGPD).

El RGPD, es un reglamento de la Unión Europea, define los datos personales como: “cualquier información relacionada con una persona física

¹⁷⁴ Asamblea Legislativa. (2011). Ley de acceso a la información pública. 6FEC6152-A946-4C2E-B232-04C3EA89FCE0.pdf (asamblea.gob.sv)

¹⁷⁵ Asamblea Legislativa. (2016). Ley especial contra delitos informáticos y conexos. DCOAD0B7-28EF-461B-991E-563CB879998F.pdf (asamblea.gob.sv)

¹⁷⁶ Santos, Sandra. Revista Factum. (2022). Nuestros datos personales están desprotegidos. Nuestros datos personales están desprotegidos - Revista Factum

¹⁷⁷ Gobierno de El Salvador. (2022). Política de ciberseguridad. (Diario Oficial No.90 Tomo. 435 del 13, publicado, 13 de mayo de 2022).

identificada o identificable”¹⁷⁸. Incluye no solo datos personales como nombres y direcciones, sino también otro tipo de datos, como direcciones IP e identificadores en línea.

El reglamento no proporciona una lista exhaustiva de lo que se encuentra excluido de los datos personales. En cambio, se centra en definir ampliamente lo que constituye datos personales. Sin embargo, reconoce que los datos anónimos (datos que no se pueden vincular a un individuo) no se consideran datos personales¹⁷⁹.

El RGPD incluye los siguientes puntos¹⁸⁰:

Responsabilidades del procesador de datos:

Cuando se utilizan servidores externos o proveedores de bases de datos, el procesador de datos debe asegurarse de que proporcionen garantías suficientes para implementar medidas técnicas y organizativas apropiadas.

Estándares de transferencia de datos: Las transferencias de datos a países fuera de la Unión Europea deben asegurar una protección adecuada de los datos. El RGPD proporciona mecanismos específicos, como las Cláusulas Contractuales Estándar o la adhesión al marco del Escudo de Privacidad UE-EE.UU. (si es aplicable).

¹⁷⁸ Comisión Europea, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)”, (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-3A32016R0679>

¹⁷⁹ ídem.

¹⁸⁰ ídem

Requisitos de seguridad de datos: Las empresas deben implementar medidas de seguridad apropiadas para proteger los datos contra el procesamiento no autorizado o ilegal y contra la pérdida, destrucción o daño accidental.

Protocolos ante brechas de datos: En caso de una brecha de datos, las empresas deben notificar a las autoridades reguladoras correspondientes y potencialmente a los sujetos de datos afectados, especialmente si la brecha representa un alto riesgo para sus derechos y libertades.

Obligaciones contractuales: Los controladores de datos deben tener contratos establecidos con sus procesadores de datos, que detallen el asunto, duración, naturaleza y propósito del procesamiento, así como las obligaciones y derechos del controlador.

(II) LEY GRAMM-LEACH-BLILEY (LGLB).

La LGLB, es una ley federal de los Estados Unidos aplicable principalmente a las instituciones financieras, define la información personal no pública como “información financiera personalmente identificable” e incluye información que los consumidores proporcionan para obtener un producto o servicio financiero. Excluye la información públicamente disponible, como la información en registros públicos, y cualquier dato que esté cifrado, asegurado o hecho anónimo¹⁸¹.

La LGLB incluye las siguientes instrucciones¹⁸²:

Regla de salvaguardia: Las instituciones financieras deben tener un plan de seguridad escrito que explique cómo la empresa protege la información personal no pública de los clientes, incluyendo cuando se utilizan proveedores de servicios externos.

Supervisión de proveedores de servicios: Las empresas deben asegurarse de que sus proveedores de servicios puedan mantener salvaguardias apropiadas para la información del cliente y están contractualmente obligados a implementar y mantener dichas salvaguardias.

Gestión de riesgos: Se requiere la realización regular de pruebas y monitoreo de la efectividad de las salvaguardias. Esto también debe cubrir servidores externos y proveedores de base de datos.

Programa de seguridad de la información: Las instituciones financieras deben desarrollar, implementar y mantener un programa integral de seguridad de la información diseñado para asegurar la seguridad y confidencialidad de la información del cliente.

Seguridad de la información del cliente: Las empresas deben proteger contra cualquier amenaza o peligro anticipado para la seguridad o integridad de dicha información, incluyendo en escenarios de gestión de datos externos.

¹⁸¹ Gramm-Leach-Bliley Act of 1999. Public Law 106-102, U.S. Statutes at Large 113 (1999): 1338–1481 <https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf>. <https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf>

¹⁸² ídem

B. CHIVO WALLET: POLÍTICA DE PRIVACIDAD, TÉRMINOS Y CONDICIONES

Chivo Wallet es la billetera electrónica desarrollada por el GOES en 2021 disponible para android y ios¹⁸³. Aunque Chivo Wallet opera como una entidad privada bajo la ley comercial,¹⁸⁴ se encuentra estrechamente vinculada a las operaciones gubernamentales y financiadas con dinero público.¹⁸⁵ En este sentido, es necesario aclarar si la Ley de Acceso a la Información Pública (LAIP) se aplica a los datos utilizados por Chivo Wallet.

El artículo 7 de la LAIP estipula que las entidades que manejan recursos públicos, información, o realizan funciones estatales están obligadas a proporcionar acceso a la información relacionada con la administración de dichos recursos¹⁸⁶. Este artículo establece que las empresas de economía mixta y las personas naturales o jurídicas que utilicen recursos o información pública o realicen actos de la función estatal deben permitir el acceso a la información relacionada con la administración de los fondos o la función pública asignada.¹⁸⁷

Al referirse a la información privada la LAIP señala, que es la relacionada con una persona identificada o identificable, e incluye detalles como nacionalidad, domicilio, patrimonio, correo electrónico, número de teléfono. También define los datos personales sensibles como aquellos relacionados con el credo, religión, origen étnico, afiliación política, salud física y mental, entre otros.

En los términos y condiciones, se menciona únicamente que se toman precauciones para proteger la información mediante sistemas de seguridad informática efectivos.¹⁸⁸ Sin embargo, no se especifican medidas de seguridad estrictas, dejando al usuario sin un conocimiento claro de cómo se protegerán sus datos, especialmente en comparación con los estándares internacionales, que más adelante se relacionarán.

La política de ciberseguridad de El Salvador establece directrices y mejores prácticas para gestionar los riesgos, incluyendo un proceso que consta de varios pasos para analizar y priorizar las brechas que pueden afectar los costos y riesgos de las organizaciones. Este marco exige que las instituciones determinen los recursos necesarios para abordar dichas brechas.

El Salvador debe cumplir con los estándares de seguridad de la información para proteger los datos personales de los usuarios. También considerar los

¹⁸³ Chivo Wallet. Descripción. <https://www.chivowallet.com/terminos-y-condiciones.html>

¹⁸⁴ Alvarado, Jimmy. El Faro. (2021). Chivo es una empresa privada financiada con fondos públicos. Chivo es una empresa privada financiada con fondos públicos (elfaro.net)

¹⁸⁵ Chivo Wallet. (s.f.). Chivo Wallet Is an Electronic Wallet Created by the Government of El Salvador for Making Payments in Dollars or Bitcoin. Inicio | Chivo Wallet

¹⁸⁶ Asamblea Legislativa. (2011). Ley de acceso a la información pública. (art.7). 6FEC6152-A946-4C2E-B232-04C3EA89FCE0.pdf (asamblea.gob.sv)

¹⁸⁷ ídem.

¹⁸⁸ Chivo Wallet.(s.f). Términos y condiciones. Términos y Condiciones | Chivo Wallet

estándares ISO: ISO/IEC 27001:2022,¹⁸⁹ sobre sistemas de gestión de seguridad de la información y protección de la privacidad, y ISO/IEC 27035-1:2023 sobre gestión de incidentes de seguridad de la información, junto con las regulaciones aplicables a los bancos y a los AV.¹⁹⁰

Otros estándares sobre seguridad de la información y protección de datos provienen de CNB-CR-07/2020 NR-23 que establece las Normas técnicas para la gestión de la seguridad de la información, aplicable a instituciones financieras¹⁹¹ y específicamente para los PSAD, a través del Reglamento de los Proveedores de Servicios de Activos Digitales, en donde se menciona que se deberán establecer procedimientos sobre la gobernanza, identificación, protección, detección, respuesta y recuperación, incluyendo realización de pruebas y simulaciones para garantizar los pilares de la seguridad de la información: confidencialidad, disponibilidad e integridad.¹⁹²

¹⁸⁹ ISO/IEC 27001:2022 is an international standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The goal is to help organizations make the information assets they hold more secure. This includes aspects of cybersecurity and privacy protection. The standard requires organizations to assess their information security risks, implement appropriate security controls, and continuously monitor and improve the effectiveness of their ISMS.

¹⁹⁰ Superintendency of Banks, Insurance, and AFP. Weekly Bulletin No. 7. Information Security and Cybersecurity: New Regulation to Promote a Secure and Reliable Environment for the Benefit of Users of Supervised Systems [Seguridad de la información y ciberseguridad: nuevo reglamento para promover un entorno seguro y confiable en beneficio de los usuarios de los sistemas supervisados]. See here. March 2021. Accessed on June 28, 2024.

¹⁹¹ Banco Central de Reserva, "CNBCR-07/2020 NR-23 que establece las Normas técnicas para la gestión de la seguridad de la información", 2020. <https://www.bcr.gob.sv/regulaciones/upload/NRP-23.pdf>

¹⁹² CNAD, "Reglamento de Proveedores de Activos Digitales", 2023. <https://cnad.gob.sv/es/libreria-de-documentacion/marco-legal/#-flipbook-reglamento-de-proveedores-de-servicios-de-activos-digitales-2023-08-11-esp/1/>

C. BILLETERAS DE ACTIVOS VIRTUALES

Como se explicó en capítulos anteriores, es necesario poder identificar a las personas políticamente expuestas al realizar actividades con los PSAD. Las carteras digitales están sometiendo cada vez más a escrutinio las actividades de los ciudadanos, pero también de ciertos grupos como los partidos políticos o los PEPs analizados en este informe para garantizar el cumplimiento de los estándares globales contra el LA. Este enfoque ayuda a mejorar las medidas de seguridad y mantener la integridad de las transacciones financieras. A medida que las regulaciones se endurecen, comprender cómo las principales carteras digitales gestionan a sus usuarios se vuelve crucial. Esta visión general destaca los enfoques de plataformas como Binance y Kraken en la regulación de transacciones que involucran a PEP, por ejemplo, demostrando su compromiso con los estándares internacionales de cumplimiento. A continuación, algunos comentarios específicos de cómo abordan este tema en particular:

Binance: Binance es una casa de cambio y exige que todos los usuarios se sometan a una verificación de identidad para reforzar la seguridad de la cuenta y asegurar el cumplimiento de los requisitos regulatorios aplicables. Como parte de su proceso interno, se solicita a los usuarios que revelen si son PEP¹⁹³. Aquellos identificados como PEP deben completar un formulario específico detallando su estatus y también pueden ser solicitados para proporcionar documentación que sustente su Fuente de Riqueza (SOW por sus siglas en inglés).

¹⁹³ Binance, "How to complete de source of health declaration", <https://www.binance.com/en/support/faq/how-to-complete-the-source-of-wealth-declaration-c22109193d1247b3af1027e-72fa0d5b7>

Kraken: Es una casa de cambio que al igual que Binance, Kraken incorpora la identificación de PEP en sus procedimientos de KYC. La plataforma se alinea con la definición de PEP del GAFI, incluyendo a individuos que hayan ocupado anteriormente roles públicos significativos. Kraken requiere que las PEP proporcionen documentación extensa, incluyendo estados financieros y de activos, para verificar sus identidades y evaluar los riesgos potenciales. Este enfoque refuerza el compromiso de Kraken con la prevención del uso financiero indebido y la mejora de la transparencia¹⁹⁴.

Estas medidas ilustran los pasos proactivos que toman las carteras digitales para gestionar los riesgos asociados con las PEP, asegurando que operen dentro de los límites de las regulaciones financieras internacionales.

D. ANÁLISIS COMPARATIVO DE BILLETERAS DE AV

Una revisión de las políticas de privacidad de varias plataformas revela importantes discrepancias en el cumplimiento de los estándares de protección de datos. A continuación, un breve análisis del desarrollo y uso de información por parte de billeteras de AV que operan en El Salvador.

Blink: Sus términos permiten el uso amplio de datos, tanto restringidos como no restringidos, para diversos fines, incluidos los traspasos a terceros¹⁹⁵. Los términos especifican que se pueden utilizar servidores de

terceros que cumplan con estándares internacionales de seguridad como ISO/IEC 27001:2013, PCI-DSS, PII y HIPAA. También permiten la revocación de estas autorizaciones de manera no restrictiva y proporcionan una dirección de correo electrónico para ejercer los derechos de protección de datos¹⁹⁶.

Strike: Sus políticas de privacidad son detalladas, cubriendo el uso de información personal, la transferencia de datos a terceros, la duración de la retención y los detalles de acceso a los datos. Indican que cualquier solicitud de terceros no cubierta en las políticas de privacidad estará sujeta al consentimiento del usuario¹⁹⁷. Los términos también mencionan el uso de cookies y reconocen posibles vulnerabilidades en la transmisión de datos, aunque afirman cumplir con las regulaciones locales¹⁹⁸.

DitoBanx: Describe brevemente el uso de la información personal recopilada y el control de los usuarios sobre sus datos, incluida la opción de recibir o no comunicaciones¹⁹⁹. Sin embargo, no se muestra información detallada sobre la gestión y el intercambio de datos, lo que plantea un riesgo potencial para la seguridad de los datos de los usuarios²⁰⁰.

¹⁹⁴ Kraken "Political Exposed Person-self declaration", <https://support.kraken.com/hc/en-us/articles/politically-exposed-person-pep-self-declaration-definitions>

¹⁹⁵ Blink, Política de Privacidad (2024). <https://es.blink.sv/en/privacy-policy>

¹⁹⁶ Blink, Política de Privacidad (2024). <https://es.blink.sv/en/privacy-policy>

¹⁹⁷ Strike, Aviso de Privacidad de Strike (2023). <https://strike.me/legal/privacy/>

¹⁹⁸ Strike, Aviso de Privacidad de Strike (2023). <https://strike.me/legal/privacy/>

¹⁹⁹ DitoBanx, Política de Privacidad (2024). <https://ditobanx.com/polica-de-privacidad/>

²⁰⁰ DitoBanx, Política de Privacidad (2024). <https://ditobanx.com/polica-de-privacidad/>

Bitfinex: Proporciona una cuenta más detallada de sus prácticas de datos, incluidos los tipos de información recopilada, los fines de la recopilación de datos, los detalles del almacenamiento, las políticas de intercambio y las medidas de seguridad²⁰¹. También aclara la base legal para el procesamiento de datos y cómo los usuarios pueden ejercer sus derechos, demostrando un estándar más alto de protección de datos²⁰².

Los PSAD cumplen con estándares de protección de datos internacionales, por la misma naturaleza de su operación transnacional, la cual permite que personas usuarias de diferentes jurisdicciones puedan utilizar sus productos y servicios.

²⁰¹ Bitfinex, Bitfinex Privacy Statement (2024), <https://www.bitfinex.com/legal/privacy/>

²⁰² Bitfinex, Bitfinex Privacy Statement (2024), <https://www.bitfinex.com/legal/privacy/>

RECOMENDACIONES

A continuación, se comparten algunas recomendaciones para abordar las principales temáticas del reporte:

RECOMENDACIONES PARA CONTRARRESTAR DELITOS FINANCIEROS

- Educar a la población salvadoreña y a los usuarios sobre finanzas y tecnología, destacando los riesgos de la exposición de datos personales en plataformas financieras y de AV, para prevenir delitos como las estafas o fraudes informáticos.
- Fomentar estándares estrictos de seguridad de la información en el ecosistema financiero y tecnológico en El Salvador, aplicando sanciones efectivas en caso de incumplimiento.
- Implementar medidas basadas en riesgos y respuesta ante brechas de seguridad de la información en los PSAD y PSB, con detección en tiempo real de amenazas y medidas de seguridad que refuercen la confianza de los inversionistas.

RECOMENDACIONES PARA PREVENIR EL LA/FT/PADM

- Profundizar en un enfoque basado en riesgo sobre la utilización de Bitcoin y otros activos digitales dentro de El Salvador, incluyendo las monedas estables, activos digitales subyacentes y derivados con el fin de mitigar el LDA/FT.

- Fortalecer el conocimiento de las autoridades en prevención, investigación, persecución y enjuiciamiento de delitos relacionados con AV, enfocados en las etapas de lavado de dinero, tipologías utilizadas por los delincuentes y el financiamiento del terrorismo.

- Desarrollar guías o manuales en armonía con la legislación penal y procesal penal para el congelamiento de AV por parte de la Policía y FGR, así como socializar con el sector justicia dichas prácticas desde un enfoque de cooperación judicial internacional.

- Fortalecer las capacidades técnicas de las autoridades como la Policía, FGR y la Corte Suprema de Justicia, en la gestión de evidencia digital relacionada con delitos habilitados por los AV.

- Promover la cooperación entre el sector privado-público para mejorar la comunicación en la investigación y persecución de los delitos y faltas, compartiendo buenas prácticas y lecciones aprendidas.

- Sugerir a los supervisores de los PSB y PSAD elaborar guías claras para prevenir delitos financieros en la industria de AV y como parte del uso de sus plataformas, considerando estándares internacionales e identificación de banderas rojas sobre patrones, anonimidad, origen de los fondos, y otros aspectos para contrarrestar el LA/FT.

- Realizar consultas públicas a los diferentes sectores en la adopción de regulaciones sobre finanzas y tecnología, con el fin de mejorar el enfoque basado en riesgos que permita la prevención e identificación del LA/FT.

- Fomentar la colaboración regulatoria entre el sector financiero tradicional y los PSAD/PSB en temas de LA/FT.

- Garantizar que la entidad supervisora en materia electoral pueda realizar una supervisión de las PEP en las plataformas digitales para cumplir con estándares internacionales, asegurando la identificación de usuarios y origen de AV.

- Establecer lineamientos claros para la implementación de “la regla del viajero” en el sector de los PSAD/PSB, por parte de la UIF y en coordinación con el sector financiero tradicional.

RECOMENDACIONES SOBRE FINANCIAMIENTO POLÍTICO

- Dotar al TSE de recursos humanos, tecnológicos, y financieros suficientes para supervisar y auditar todas las donaciones, especialmente las realizadas a través de AV.

- Actualizar el marco normativo para regular el uso de AV en el financiamiento político. Establecer controles claros y asegurar que los entes supervisores, como la TSE, MH, CCR y la CNAD, cumplan con las recomendaciones del GAFI y los estándares internacionales.

- Fortalecer la coordinación entre supervisores del proceso electoral, el TSE, MH, CCR, la CNAD, y los PSAD/PSB, con el fin de garantizar una colaboración efectiva en la identificación de banderas rojas en el ámbito político.

- Establecer lineamientos de control sobre donaciones de AV para los partidos políticos, garantizando el cumplimiento de la Ley de Partidos Políticos (LPP) y la normativa relacionada al LA/FT.

RECOMENDACIONES SOBRE TOKENIZACIÓN DE ACTIVOS DEL MUNDO REAL

- Crear un ecosistema y normativo seguro para prevenir fraudes y garantizar la seguridad jurídica de los inversionistas dentro del proceso de tokenización o de ofertas de AV.

- Aumentar el conocimiento y capacitación sobre la tokenización y emisión de AV para fomentar la confianza en las tecnologías financieras. Es importante establecer y definir los riesgos asociados con la inversión en activos digitales de manera accesible y comprensible para los inversionistas.

- Promover espacios de coordinación entre los diversos sectores involucrados en la emisión de activos digitales, para compartir buenas prácticas en la prevención de delitos financieros.

- Contrarrestar vulneraciones de seguridad conforme a los estándares internacionales en la seguridad de la información dentro de la infraestructura de intercambio de tokens, con el fin de prevenir delitos financieros.

- Establecer las oportunidades de tokenización en los diferentes sectores, como la construcción, productos agrícolas, fondos y deudas, aplicando enfoques basados en riesgos específicos de cada sector.

- Fomentar el conocimiento sobre la utilización de monedas estables, proporcionando información clara y abordando su relación con los riesgos asociados al LA/FT.

- Reforzar el conocimiento técnico sobre AV y el proceso de tokenización por parte de las autoridades competentes para contrarestar delitos financieros u otro tipo de ciberdelitos.

RECOMENDACIONES SOBRE PROTECCIÓN DE DATOS PERSONALES

- Exigir el cumplimiento de la normativa en materia de seguridad de la información y la implementación de la ISO/IEC 27001:2022. Las agencias gubernamentales pueden utilizar este estándar para salvaguardar los datos sensibles de los ciudadanos, asegurando el cumplimiento de las regulaciones nacionales e internacionales mientras mejoran la confianza pública en los servicios gubernamentales. Las instituciones financieras también se beneficiarían de este estándar al asegurar los datos financieros de los clientes, prevenir fraudes y adherirse a regulaciones financieras estrictas.

- Seguir los estándares de la seguridad de la información para proteger la infraestructura y datos de clientes por parte de los PSAD y PSB, incluyendo transacciones, para ello se recomienda realizar pruebas controladas por parte de expertos en seguridad de la información.



GLOBAL FINANCIAL INTEGRITY



CYRUS R. VANCE CENTER
FOR INTERNATIONAL JUSTICE