CRYPTADIUM

POLÍTICA AML/KYC

v4.0 | 26 de abril de 2026 | DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.)

En caso de conflicto entre la versión en español y cualquier traducción al inglés, prevalecerá la versión en español.

CRYPTADIUM

AML/KYC POLICY

v4.0 | 26 April 2026 | DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.)

In the event of conflict between the Spanish and English versions, the Spanish version shall prevail.

1. OBJETIVO, ÁMBITO Y DECLARACIÓN DE APETITO AL RIESGO

Esta Política AML/KYC establece el marco de prevención del lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva (AML/CFT/FP) de DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.), operando como CRYPTADIUM, conforme a la LEPLAF (DL 426/2025), las Recomendaciones GAFILAT para Activos Virtuales y VASPs, y la LBAD (DL 643/11 enero 2023). Cryptadium opera exclusivamente servicios de procesamiento de pagos en Bitcoin (BTCSP, Licencia CNAD N.° 68af4cefe8a00a3181b9878b).

> **Declaración de Apetito al Riesgo AML/CFT/FP: Cryptadium mantiene un apetito al riesgo AML/CFT/FP BAJO. Cryptadium no acepta Comerciantes ni Transacciones que presenten indicios de lavado de activos, financiamiento del terrorismo, financiamiento de la proliferación de armas de destrucción masiva o evasión de sanciones. El programa AML/CFT/FP ha sido aprobado por el Director de DUALPAY, S.A. de C.V. y es revisado y aprobado anualmente por la alta dirección.**

Evaluación institucional de riesgos: Cryptadium realizará una evaluación institucional de riesgos AML/CFT/FP al menos una vez al año y cuando existan cambios materiales en productos, jurisdicciones, clientes, canales, tecnología, tipologías de riesgo o normativa aplicable. Esta Política aplica a todas las operaciones de Cryptadium como BTCSP, todos los Comerciantes y sus directores/UBOs/representantes, todas las Transacciones

1. OBJECTIVE, SCOPE AND RISK APPETITE STATEMENT

This AML/KYC Policy establishes the anti-money laundering, counter-financing of terrorism and counter-proliferation financing (AML/CFT/PF) framework of DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.), operating as CRYPTADIUM, pursuant to the LEPLAF (DL 426/2025), GAFILAT Recommendations for Virtual Assets and VASPs, and the LBAD (DL 643/11 January 2023). Cryptadium exclusively operates Bitcoin payment processing services (BTCSP, CNAD Licence No. 68af4cefe8a00a3181b9878b).

> **AML/CFT/PF Risk Appetite Statement: Cryptadium maintains a LOW AML/CFT/PF risk appetite. Cryptadium does not accept Merchants or Transactions presenting indications of money laundering, terrorist financing, proliferation financing or sanctions evasion. The AML/CFT/PF programme has been approved by the Director of DUALPAY, S.A. de C.V. and is reviewed and approved annually by senior management.**

Institutional risk assessment: Cryptadium shall conduct an enterprise-wide AML/CFT/PF risk assessment at least annually and upon material changes in products, jurisdictions, customers, channels, technology, risk typologies or applicable regulation. This Policy applies to all Cryptadium operations as a BTCSP, all Merchants and their

en Bitcoin procesadas a través de la Plataforma, y todo el personal, directivos y asesores externos de Cryptadium.	directors/UBOs/representatives, all Bitcoin Transactions processed through the Platform, and all Cryptadium staff, directors and external advisors.

2. MARCO NORMATIVO

2. REGULATORY FRAMEWORK

• LEPLAF (DL 426/2025): Ley Especial para la Prevención, Control y Sanción del Lavado de Activos, el Financiamiento del Terrorismo y el Financiamiento de la Proliferación de Armas de Destrucción Masiva — ley AML/CFT/FP principal de El Salvador, en vigor desde 2025.	• LEPLAF (DL 426/2025): Special Law for the Prevention, Control and Sanction of Money Laundering, Terrorist Financing and Proliferation Financing — El Salvador's principal AML/CFT/PF law, in force since 2025.
• LBAD (DL 643/11 enero 2023): Ley de Emisión de Activos Digitales — regula la licencia BTCSP y obligaciones de cumplimiento para proveedores de servicios de activos digitales.	• LBAD (DL 643/11 January 2023): Digital Asset Issuance Law — regulates the BTCSP licence and compliance obligations for digital asset service providers.
• Ley Bitcoin (DL 57/2021 + Decreto 199/30 enero 2025): Bitcoin como medio de pago con aceptación voluntaria en El Salvador.	• Bitcoin Law (DL 57/2021 + Decree 199/30 January 2025): Bitcoin as a means of payment with voluntary acceptance in El Salvador.
• GAFILAT Recomendaciones 10, 15, 16, 20 y 40 para VASPs: KYC, activos virtuales, Travel Rule, ROS, cooperación internacional.	• GAFILAT Recommendations 10, 15, 16, 20 and 40 for VASPs: KYC, virtual assets, Travel Rule, ROS, international cooperation.
• OFAC/ONU/UE/UK: regímenes internacionales de sanciones, incluyendo la regla del 50% de OFAC para propiedad y control directo e indirecto.	• OFAC/UN/EU/UK: international sanctions regimes, including the OFAC 50% rule for direct and indirect ownership and control.
• UIF (Unidad de Investigación Financiera de la Fiscalía General de la República): unidad de inteligencia financiera competente de El Salvador — receptor de ROS (Reportes de Operación Sospechosa).	• UIF (Unidad de Investigación Financiera de la Fiscalía General de la República): El Salvador's competent financial intelligence unit — recipient of ROS (Reportes de Operación Sospechosa).

3. GOBERNANZA AML/CFT/FP

3. AML/CFT/PF GOVERNANCE

3.1 Oficial de Cumplimiento AML (MLRO)

Cryptadium designa un Oficial de Cumplimiento AML (MLRO) con autoridad e independencia suficientes de las funciones comerciales y operativas, sin conflicto de interés, que reporta directamente al Director. El MLRO ejercerá sus funciones sin interferencia y contará con protección contra represalias internas por decisiones de cumplimiento. Responsabilidades: diseñar, implementar y supervisar el programa AML/CFT/FP; recibir y analizar alertas internas; determinar y presentar ROS a la UIF; capacitar al personal; elaborar informe anual de cumplimiento al Director. Controles de integridad del personal: Cryptadium implementará controles razonables de idoneidad, antecedentes, sanciones y conflictos de interés para el personal en funciones sensibles de cumplimiento, operaciones, tecnología y acceso a datos o fondos.

3.2 Tres Líneas de Defensa

- Primera línea — Operaciones y Negocio: aplicación diaria de controles KYC/AML/CFT/FP, onboarding, monitoreo, detección de alertas.
- Segunda línea — MLRO y Compliance: supervisión independiente, políticas, formación, análisis de alertas, reporte.
- Tercera línea — Auditoría Independiente: revisión y auditoría del programa AML mínimo anual. Estándar mínimo recomendado: auditoría externa independiente.

3.1 AML Compliance Officer (MLRO)

Cryptadium designates an AML Compliance Officer (MLRO) with sufficient authority and independence from commercial and operational functions, without conflict of interest, reporting directly to the Director. The MLRO shall act without interference and shall be protected against internal retaliation for compliance decisions. Responsibilities: design, implement and supervise the AML/CFT/PF programme; receive and analyse internal alerts; determine and file ROS with the UIF; train staff; prepare annual compliance report to the Director. Personnel integrity controls: Cryptadium shall implement reasonable fitness, background, sanctions and conflict-of-interest checks for personnel in sensitive compliance, operations, technology and data or funds access roles.

3.2 Three Lines of Defence

- First line — Operations and Business: day-to-day KYC/AML/CFT/PF controls, onboarding, monitoring, alert detection.
- Second line — MLRO and Compliance: independent oversight, policies, training, alert analysis, reporting.
- Third line — Independent Audit: AML programme review and audit at minimum annually. Recommended minimum standard: independent external audit.

4. DEBIDA DILIGENCIA — KYC/CDD/EDD

4.1 Actividades Absolutamente Prohibidas

> **Queda expresamente prohibido establecer o mantener relaciones comerciales con entidades o actividades que requieran licencia, registro o autorización regulatoria y que no cuenten con dicha autorización en su jurisdicción aplicable. Estos casos no podrán ser mitigados mediante EDD y serán rechazados automáticamente, sin excepción.**

4. CUSTOMER DUE DILIGENCE — KYC/CDD/EDD

4.1 Absolutely Prohibited Activities

> **It is expressly prohibited to establish or maintain business relationships with entities or activities that require a licence, registration or regulatory authorisation and do not hold such authorisation in the applicable jurisdiction. Such cases cannot be mitigated through EDD and shall be automatically rejected, without exception.**

4.2 Debida Diligencia Estándar (CDD)	4.2 Standard Customer Due Diligence (CDD)
Aplicable a todos los Comerciantes en el onboarding y durante toda la relación (KYC perpetuo — actualización per nivel de riesgo: alto: mínimo anual; medio: bienal; bajo: trienal). Incluye: verificación de persona jurídica (escritura de constitución, certificado de vigencia, NIT, matrícula de comercio, licencias sectoriales aplicables); identificación y verificación de UBOs (umbral interno ≥10%; puede ser más estricto per análisis de riesgo): nombre completo, fecha de nacimiento, nacionalidad, documento de identidad, dirección; verificación del representante legal (poderes, identidad, autorización vigente); fuente de fondos y riqueza (cuando corresponda per perfil de riesgo); descripción del modelo de negocio (productos, geografía, canales, volumen estimado); declaración PEP/sanciones actualizada para todos los directores, UBOs y representantes.	Applied to all Merchants at onboarding and throughout the relationship (perpetual KYC — update per risk level: high: minimum annually; medium: biennially; low: triennially). Includes: legal entity verification (articles of incorporation, good standing certificate, NIT, commercial registration, applicable sector licences); UBO identification and verification (internal threshold ≥10%; may be stricter per risk analysis): full name, date of birth, nationality, identity document, address; legal representative verification (powers of attorney, identity, current authorisation); source of funds and wealth (where applicable per risk profile); business model description (products, geography, channels, estimated volume); updated PEP/sanctions declaration for all directors, UBOs and representatives.
4.3 Debida Diligencia Reforzada (EDD)	**4.3 Enhanced Due Diligence (EDD)**
Obligatoria en: sectores de alto riesgo aprobados (casinos online, apuestas deportivas, contenido para adultos, exchanges de criptoactivos licenciados); estructuras corporativas complejas u opacas; PEPs y RCAs; resultados positivos o ambiguos en screening de sanciones; volúmenes inusualmente altos o patrones atípicos. La EDD incluye: información adicional verificada sobre fuente de riqueza; verificación reforzada de terceros independientes; aprobación expresa del MLRO; revisión más frecuente; aprobación del Director para sectores de máximo riesgo.	Mandatory in: approved high-risk sectors (online casinos, sports betting, adult content, licensed crypto exchanges); complex or opaque corporate structures; PEPs and RCAs; positive or ambiguous sanctions screening; unusually high volumes or atypical patterns. EDD includes: additional verified source of wealth information; enhanced independent third-party verification; express MLRO approval; more frequent review; Director approval for maximum-risk sectors.

5. MONITOREO CONTINUO Y ANÁLISIS DE TRANSACCIONES	5. ONGOING MONITORING AND TRANSACTION ANALYSIS
• Blockchain analytics: herramientas de análisis blockchain actualizadas periódicamente — detección de exposición a mixers, darknet, ransomware y jurisdicciones sancionadas.	• Blockchain analytics: regularly updated blockchain analytics tools — detection of exposure to mixers, darknet, ransomware and sanctioned jurisdictions.
• Monitoreo transaccional automatizado: detección de smurfing/estructuración, volúmenes anómalos, frecuencia inusual, patrones incompatibles con el perfil declarado.	• Automated transaction monitoring: detection of smurfing/structuring, anomalous volumes, unusual frequency, patterns inconsistent with the declared profile.

• Actualización periódica del perfil de riesgo del Comerciante per nivel de riesgo asignado.	• Periodic update of Merchant risk profile per assigned risk level.
• Screening continuo de sanciones: OFAC/ONU/UE/UK y listas nacionales; regla del 50% directa e indirecta; actualización en tiempo real o con la frecuencia mínima recomendada por las autoridades pertinentes.	• Continuous sanctions screening: OFAC/UN/EU/UK and national lists; 50% rule direct and indirect; real-time or minimum-frequency updates per relevant authorities.

6. TRAVEL RULE (GAFILAT RECOMENDACIÓN 16)

6. TRAVEL RULE (GAFILAT RECOMMENDATION 16)

Per instrucciones de la UIF y directrices de la CNAD para VASPs, Cryptadium recopila, verifica y transmite la información Travel Rule en cada Transacción de activos virtuales (Bitcoin), sin perjuicio de umbrales específicos que puedan establecer la UIF o la CNAD en sus instrucciones vigentes:	Per UIF instructions and CNAD VASP guidelines, Cryptadium collects, verifies and transmits Travel Rule information in each virtual asset Transaction (Bitcoin), without prejudice to thresholds that may be set by UIF or CNAD in their current instructions:
• Información del originador: nombre completo, wallet/cuenta, dirección física, documento de identidad y fecha de nacimiento (o número de cliente asignado por el VASP), país de origen.	• Originator information: full name, wallet/account, physical address, identity document and date of birth (or VASP-assigned customer number), country of origin.
• Información del beneficiario: nombre completo, wallet/cuenta del beneficiario y, cuando sea requerido por normativa aplicable, instrucciones UIF/CNAD o enfoque basado en riesgo, también dirección física y documento de identidad.	• Beneficiary information: full name, beneficiary wallet/account, and where required by applicable regulation, UIF/CNAD instructions or risk-based approach, also physical address and identity document.
Debida diligencia de VASPs contrapartes y transmisión segura: Cryptadium realizará debida diligencia sobre VASPs contrapartes antes de transmitir información Travel Rule y utilizará canales seguros, cifrados y verificables que garanticen la confidencialidad, integridad y trazabilidad de la información transmitida. Para billeteras no custodiadas (unhosted wallets) y no-VASPs: enfoque basado en riesgo — verificación adicional de identidad, EDD reforzada, rechazo si riesgo elevado per determinación del MLRO.	Counterparty VASP due diligence and secure transmission: Cryptadium shall conduct due diligence on counterparty VASPs prior to transmitting Travel Rule information and shall use secure, encrypted and verifiable channels ensuring confidentiality, integrity and traceability. For unhosted wallets and non-VASPs: risk-based approach — additional identity verification, enhanced EDD, rejection where risk is elevated per MLRO determination.

7. ROS Y TIPPING-OFF

7. ROS AND TIPPING-OFF

Per LEPLAF (DL 426/2025), Cryptadium está legalmente obligada a presentar Reportes de Operación Sospechosa (ROS) ante la UIF (Unidad de Investigación Financiera de la Fiscalía General de la República) cuando existan indicios razonables de ML/TF/FP u otra actividad delictiva relacionada. Procedimiento: empleado detecta actividad sospechosa → reporta inmediatamente al MLRO (sin revelar sospecha al investigado) → MLRO analiza y documenta → determina si procede ROS → decisión documentada con justificación.

ABSOLUTAMENTE PROHIBIDO per LEPLAF: revelar a la persona investigada, al Comerciante o a terceros no autorizados: (a) que se ha presentado o se presentará un ROS; (b) que existe una investigación AML/CFT/FP; (c) que Cryptadium ha bloqueado, rechazado o está revisando una Transacción por motivos AML. Esta prohibición aplica a todos los empleados, directivos, asesores y proveedores. La violación puede constituir delito penal per LEPLAF.

Per LEPLAF (DL 426/2025), Cryptadium is legally required to file Suspicious Activity Reports (ROS) with the UIF when there are reasonable indications of ML/TF/PF or related criminal activity. Procedure: employee detects suspicious activity → immediately reports to MLRO (without disclosing to investigated person) → MLRO analyses and documents → determines whether ROS is warranted → decision documented with justification.

ABSOLUTELY PROHIBITED per LEPLAF: disclosing to the investigated person, the Merchant or any unauthorised third party: (a) that an ROS has been or will be filed; (b) that an AML/CFT/PF investigation exists; (c) that Cryptadium has blocked, rejected or is reviewing a Transaction for AML reasons. This prohibition applies to all employees, directors, advisors and providers. Violation may constitute a criminal offence under LEPLAF.

8. SANCIONES INTERNACIONALES

Cryptadium mantiene un programa integral de cumplimiento de sanciones: screening continuo y sistemático contra OFAC/ONU/UE/UK y listas nacionales aplicables de El Salvador; aplicación de la regla del 50% de OFAC y equivalentes ONU/UE/UK para propiedad y control directo e indirecto; actualización inmediata ante cambios en listas. Los bloqueos o retenciones de fondos se aplicarán de forma preventiva, proporcional y basada en riesgo, sin constituir confiscación ni transferencia de propiedad, y estarán sujetos a revisión continua y a las instrucciones de la autoridad competente conforme a la LEPLAF y normativa de sanciones aplicable. El Comerciante tiene la obligación contractual de notificar inmediatamente a compliance@cryptadium.com si él, sus directores, UBOs o contrapartes pasan a ser Personas Sancionadas.

8. INTERNATIONAL SANCTIONS

Cryptadium maintains a comprehensive sanctions compliance programme: continuous and systematic screening against OFAC/UN/EU/UK and applicable El Salvador national lists; application of the OFAC 50% rule and UN/EU/UK equivalents for direct and indirect ownership and control; immediate update upon list changes. Fund blocks or holds shall be applied on a preventive, proportionate and risk-based basis, shall not constitute confiscation or transfer of ownership, and shall be subject to ongoing review and to instructions from competent authorities under LEPLAF and applicable sanctions laws. The Merchant has a contractual obligation to immediately notify compliance@cryptadium.com if it, its directors, UBOs or counterparties become Sanctioned Persons.

9. CONSERVACIÓN Y CAPACITACIÓN

9. RETENTION AND TRAINING

Per LEPLAF Art. 12: MÍNIMO 15 AÑOS desde el fin de la relación comercial o desde la finalización de cada Transacción (lo posterior). El período de conservación podrá extenderse únicamente mientras exista una obligación legal vigente, requerimiento formal, investigación en curso o instrucción de autoridad competente (UIF, CNAD, Fiscalía). Registros conservados: expedientes KYC completos; registros de Transacciones en Bitcoin; ROS presentados y decisiones documentadas de no presentación; correspondencia con autoridades reguladoras; registros de capacitación AML del personal.	Per LEPLAF Art. 12: MINIMUM 15 YEARS from end of commercial relationship or completion of each Transaction (whichever is later). The retention period may be extended only while there is an active legal obligation, formal request, ongoing investigation or instruction from a competent authority (UIF, CNAD, Fiscalía). Retained records: complete KYC files; Bitcoin Transaction records; ROS filed and documented non-filing decisions; correspondence with regulatory authorities; staff AML training records.
Programa de capacitación: formación inicial obligatoria en onboarding; actualización anual per LEPLAF/GAFILAT; capacitación específica para roles de alto riesgo; simulacros de detección de actividades sospechosas; evaluaciones periódicas de conocimiento. Auditoría del programa AML: revisión independiente mínimo anual o ante cambios regulatorios significativos; estándar mínimo recomendado: auditoría externa independiente; resultados reportados al Director; deficiencias → planes de remediación con plazos.	Training programme: mandatory initial training at onboarding; annual update per LEPLAF/GAFILAT; specific training for high-risk roles; suspicious activity detection exercises; periodic knowledge assessments. AML programme audit: independent review at minimum annually or upon significant regulatory changes; recommended minimum standard: independent external audit; results reported to Director; deficiencies → remediation plans with defined timelines.
Versión: 4.0 | Fecha: 26 de abril de 2026 | Próx. revisión: 26 de abril de 2027 | Aprobado por: Evgenii Kudriashov, Director, DUALPAY, S.A. de C.V. | compliance@cryptadium.com | aml@cryptadium.com	*Version: 4.0 | Date: 26 April 2026 | Next Review: 26 April 2027 | Approved by: Evgenii Kudriashov, Director, DUALPAY, S.A. de C.V. | compliance@cryptadium.com | aml@cryptadium.com*