

CRYPTADIUM

POLÍTICA DE RETENCIÓN DE DATOS

v1.0 | 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.

1. OBJETIVO Y ÁMBITO

Esta Política de Retención de Datos establece los períodos de conservación aplicables a todos los datos personales y registros empresariales tratados por DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.), operando como CRYPTADIUM, conforme a la LPD (DL 144/2024), la LEPLAF (DL 426/2025), la LBAD (DL 643/11 enero 2023), y el RGPD/UK GDPR cuando apliquen extraterritorialmente. Aplica a todo el personal de Cryptadium, directivos, proveedores de servicios y terceros que traten datos en nombre de Cryptadium.

2. PRINCIPIOS GENERALES DE RETENCIÓN

- Minimización y limitación de la conservación (LPD/RGPD): los datos personales se conservan únicamente durante el tiempo necesario para los fines para los que fueron recabados, salvo que una obligación legal exija un período mayor.

CRYPTADIUM

DATA RETENTION POLICY

v1.0 | 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. OBJECTIVE AND SCOPE

This Data Retention Policy sets out the retention periods applicable to all personal data and business records processed by DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.), operating as CRYPTADIUM, pursuant to LPD (DL 144/2024), LEPLAF (DL 426/2025), LBAD (DL 643/11 January 2023), and GDPR/UK GDPR where applicable extraterritorially. Applies to all Cryptadium staff, directors, service providers and third parties processing data on Cryptadium's behalf.

2. GENERAL RETENTION PRINCIPLES

- Minimisation and storage limitation (LPD/GDPR): personal data is retained only as long as necessary for the purposes for which it was collected, unless a legal obligation requires a longer period.

<ul style="list-style-type: none"> Prevalencia de la obligación legal: cuando una ley imperativa (especialmente la LEPLAF) exija un período de retención mínimo, dicho período prevalece sobre el principio de minimización y sobre cualquier solicitud de supresión del titular. 	<ul style="list-style-type: none"> Prevalence of legal obligation: where a mandatory law (especially LEPLAF) requires a minimum retention period, that period prevails over the minimisation principle and any data subject erasure request.
<ul style="list-style-type: none"> Legal hold / Litigation hold: antes de cualquier eliminación, Cryptadium verificará si existe legal hold, litigation hold, investigación regulatoria, requerimiento de autoridad o procedimiento pendiente que requiera conservación adicional. La eliminación quedará suspendida hasta la resolución del hold. 	<ul style="list-style-type: none"> Legal hold / Litigation hold: before any deletion, Cryptadium shall verify whether there is a legal hold, litigation hold, regulatory investigation, authority request or pending proceeding requiring additional retention. Deletion shall be suspended until the hold is resolved.
<ul style="list-style-type: none"> Eliminación segura: al vencer el período de retención y verificada la ausencia de holds, los datos son eliminados de forma segura e irreversible (borrado seguro, destrucción física, o anonimización irreversible). Las copias de seguridad se eliminarán conforme a ciclos normales de eliminación segura, siempre que permanezcan protegidas y no se utilicen para otros fines. 	<ul style="list-style-type: none"> Secure deletion: upon expiry of the retention period and verified absence of holds, data is securely and irreversibly deleted (secure erasure, physical destruction, or irreversible anonymisation). Backups shall be deleted according to normal secure deletion cycles, provided they remain protected and are not used for other purposes.

3. TABLA DE PERÍODOS DE RETENCIÓN

3. RETENTION PERIODS TABLE

3.1 Datos AML/CFT/FP — LEPLAF Art. 12 (MÍNIMO 15 AÑOS)

3.1 AML/CFT/PF Data — LEPLAF Art. 12 (MINIMUM 15 YEARS)

<p>Los siguientes datos están sujetos al período mínimo obligatorio de 15 AÑOS per LEPLAF Art. 12, que prevalece sobre cualquier otro plazo y sobre el derecho de supresión:</p>	<p>The following data is subject to the mandatory minimum 15-YEAR period per LEPLAF Art. 12, which prevails over any other timeframe and the right to erasure:</p>
<ul style="list-style-type: none"> Expedientes KYC completos de Comerciantes y sus directores, UBOs y representantes: 15 años desde el fin de la relación comercial. 	<ul style="list-style-type: none"> Complete KYC files of Merchants and their directors, UBOs and representatives: 15 years from end of commercial relationship.
<ul style="list-style-type: none"> Registros completos de Transacciones en Bitcoin (fecha, monto, wallets, partes, estado, comisiones): 15 años desde la fecha de la Transacción. 	<ul style="list-style-type: none"> Complete Bitcoin Transaction records (date, amount, wallets, parties, status, fees): 15 years from the Transaction date.
<ul style="list-style-type: none"> Registros de monitoreo transaccional y alertas AML (incluyendo alertas investigadas y cerradas sin ROS): 15 años desde la fecha del evento. 	<ul style="list-style-type: none"> Transaction monitoring records and AML alerts (including alerts investigated and closed without ROS): 15 years from the event date.
<ul style="list-style-type: none"> Reportes de Operación Sospechosa (ROS) presentados a la UIF y decisiones documentadas de no presentación de ROS: 15 años desde la presentación o decisión. 	<ul style="list-style-type: none"> Suspicious Activity Reports (ROS) filed with the UIF and documented non-filing decisions: 15 years from filing or decision.

<ul style="list-style-type: none"> Registros de screening de sanciones y resultados: 15 años desde la fecha del screening. 	<ul style="list-style-type: none"> Sanctions screening records and results: 15 years from the screening date.
<ul style="list-style-type: none"> Correspondencia con autoridades reguladoras (CNAD, UIF, Fiscalía, IAIP, ACE) relacionada con AML/CFT/FP: 15 años desde la última comunicación. 	<ul style="list-style-type: none"> Correspondence with regulatory authorities (CNAD, UIF, Fiscalía, IAIP, ACE) related to AML/CFT/PF: 15 years from the last communication.
<h3>3.2 Datos Contractuales y de Relación Comercial</h3>	<h3>3.2 Contractual and Commercial Relationship Data</h3>
<ul style="list-style-type: none"> Contratos, acuerdos y Términos de Servicio aceptados por Comerciantes: vigencia del contrato + 10 años desde la terminación. 	<ul style="list-style-type: none"> Contracts, agreements and Terms of Service accepted by Merchants: contract term + 10 years from termination.
<ul style="list-style-type: none"> Facturas, registros contables y documentación financiera: 10 años desde su emisión o el período exigido por el Código de Comercio de El Salvador, lo que sea mayor. 	<ul style="list-style-type: none"> Invoices, accounting records and financial documentation: 10 years from issuance or the period required by El Salvador Commercial Code, whichever is greater.
<ul style="list-style-type: none"> Correspondencia comercial (emails, soporte, tickets): 5 años desde la última comunicación o cierre del caso. 	<ul style="list-style-type: none"> Commercial correspondence (emails, support, tickets): 5 years from the last communication or case closure.
<h3>3.3 Datos de Seguridad y Técnicos</h3>	<h3>3.3 Security and Technical Data</h3>
<ul style="list-style-type: none"> Logs de acceso y auditoría de sistemas: 2 años, salvo que formen parte de una investigación AML/CFT/FP activa (en cuyo caso, per LEPLAF). 	<ul style="list-style-type: none"> System access and audit logs: 2 years, unless part of an active AML/CFT/PF investigation (in which case, per LEPLAF).
<ul style="list-style-type: none"> Logs de seguridad e incidentes de ciberseguridad: 3 años desde la fecha del incidente, salvo período mayor requerido por autoridad competente. 	<ul style="list-style-type: none"> Security and cybersecurity incident logs: 3 years from the incident date, unless a longer period is required by a competent authority.
<ul style="list-style-type: none"> Registros de brechas de datos notificadas a ACE, Fiscalía y/o titulares per LPD Art. 25: 10 años desde la notificación, salvo período mayor requerido por autoridad competente. 	<ul style="list-style-type: none"> Records of data breaches notified to ACE, Fiscalía and/or data subjects per LPD Art. 25: 10 years from notification, unless a longer period is required by a competent authority.
<h3>3.4 Datos de Marketing, Cookies y Analíticas</h3>	<h3>3.4 Marketing, Cookie and Analytics Data</h3>
<ul style="list-style-type: none"> Datos analíticos y de rendimiento del sitio web, agregados, anonimizados o seudonimizados cuando corresponda: 2 años. 	<ul style="list-style-type: none"> Website analytics and performance data, aggregated, anonymised or pseudonymised where applicable: 2 years.
<ul style="list-style-type: none"> Preferencias de cookies y registros de consentimiento: 3 años desde la última actualización del consentimiento. 	<ul style="list-style-type: none"> Cookie preferences and consent records: 3 years from the last consent update.

- Listas de comunicación de marketing (con consentimiento): hasta la retirada del consentimiento, más 3 años para demostrar el cumplimiento.

- Marketing communication lists (consent-based): until consent withdrawal, plus 3 years to demonstrate compliance.

4. PROCEDIMIENTO DE REVISIÓN Y ELIMINACIÓN

4. REVIEW AND DELETION PROCEDURE

Cryptadium implementa un proceso periódico (mínimo anual) de revisión de retención que incluye: (1) identificación de datos que han alcanzado o están próximos a su período de retención máximo; (2) verificación de ausencia de legal hold, litigation hold, investigación regulatoria, requerimiento de autoridad o procedimiento pendiente; (3) autorización del responsable de la función correspondiente; (4) eliminación segura con registro documentado. Los registros de eliminación se conservan para acreditar el cumplimiento per LPD. Cada categoría de datos tendrá un responsable designado (data owner), encargado de validar los períodos de retención, autorizar la eliminación y asegurar el cumplimiento de esta Política. Se implementará, en la medida en que sea técnicamente factible, un sistema de control automatizado de retención para las categorías de datos donde sea posible.

Cryptadium implements a periodic (minimum annual) retention review process including: (1) identification of data that has reached or is approaching its maximum retention period; (2) verification of the absence of any legal hold, litigation hold, regulatory investigation, authority request or pending proceeding; (3) authorisation from the relevant function head; (4) secure deletion with documented record. Deletion records are retained to demonstrate LPD compliance. Each data category shall have a designated data owner responsible for validating retention periods, authorising deletion and ensuring compliance with this Policy. Automated retention enforcement shall be implemented where technically feasible.

Cuando un titular solicite la supresión de sus datos, Cryptadium evaluará si la solicitud puede ser atendida considerando los períodos de retención aplicables, en particular la obligación imperativa de 15 años per LEPLAF Art. 12. Se informará al titular del resultado y de las razones legales que limiten la supresión en el plazo de 30 días (LPD) o 1 mes (RGPD) con posible prórroga justificada.

When a data subject requests erasure, Cryptadium will assess whether the request can be fulfilled considering applicable retention periods, particularly the mandatory 15-year obligation under LEPLAF Art. 12. The data subject will be informed of the result and legal reasons limiting erasure within 30 days (LPD) or 1 month (GDPR) with possible justified extension.

Versión: 1.0 | Fecha: 26 de abril de 2026 | Próx. revisión: 26 de abril de 2027 | Aprobado por: Evgenii Kudriashov, Director, DUALPAY, S.A. de C.V. | dpo@cryptadium.com

Version: 1.0 | Date: 26 April 2026 | Next Review: 26 April 2027 | Approved by: Evgenii Kudriashov, Director, DUALPAY, S.A. de C.V. | dpo@cryptadium.com