CRYPTADIUM

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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.

CRYPTADIUM

INFORMATION SECURITY 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. OBJETIVO Y ÁMBITO

Esta Política de Seguridad de la Información establece los principios, controles y responsabilidades para proteger la confidencialidad, integridad y disponibilidad de la información y sistemas de 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 las obligaciones regulatorias de la CNAD y la ACE (Agencia de Ciberseguridad del Estado). Aplica a todo el personal, directivos, contratistas, proveedores de servicios y cualquier tercero con acceso a los sistemas o datos de Cryptadium. Las medidas técnicas y organizativas (TOMs) descritas en esta Política son coherentes con el Anexo C del APD/DPA v4.0.

Gobernanza de seguridad: la función de seguridad de la información es supervisada por un responsable designado (CISO o equivalente), responsable de la implementación, monitoreo y reporte del programa de seguridad al Director. El CISO o equivalente reporta directamente al Director de DUALPAY, S.A. de C.V. y tiene la autoridad necesaria para tomar decisiones de seguridad sin conflicto de interés.

1. OBJECTIVE AND SCOPE

This Information Security Policy establishes the principles, controls and responsibilities for protecting the confidentiality, integrity and availability of DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.) information and systems, operating as CRYPTADIUM, pursuant to LPD (DL 144/2024), LEPLAF (DL 426/2025), LBAD (DL 643/11 January 2023) and regulatory obligations of CNAD and ACE (Agencia de Ciberseguridad del Estado). Applies to all staff, directors, contractors, service providers and any third party with access to Cryptadium systems or data. TOMs described in this Policy are coherent with Annex C of the DPA v4.0.

2. PRINCIPIOS DE SEGURIDAD

- Confidencialidad: la información es accesible únicamente para personas autorizadas con necesidad legítima de acceso (need-to-know).
- Integridad: la información se mantiene exacta, completa y protegida contra modificaciones no autorizadas.
- Disponibilidad: los sistemas y datos están disponibles para usuarios autorizados cuando se necesiten, con niveles de servicio conforme al SLA vigente.
- Privacidad por diseño (Privacy by Design): los principios de protección de datos (LPD/RGPD) se incorporan en el diseño de sistemas y procesos desde el inicio.
- Mínimo privilegio: los accesos se otorgan con el nivel mínimo necesario para desempeñar las funciones autorizadas.

2. SECURITY PRINCIPLES

- Confidentiality: information is accessible only to authorised persons with a legitimate need to know.
- Integrity: information is maintained accurate, complete and protected against unauthorised modification.
- Availability: systems and data are available to authorised users when needed, at service levels per the applicable SLA.
- Privacy by design: data protection principles (LPD/GDPR) are incorporated into system and process design from the outset.
- Least privilege: access is granted at the minimum level necessary to perform authorised functions.

3. CONTROLES TÉCNICOS DE SEGURIDAD (TOMs)

- Cifrado: datos en tránsito protegidos con TLS 1.2 o superior; datos en reposo cifrados con AES-256 o equivalente.
- Control de acceso: RBAC (Role-Based Access Control); MFA (autenticación multifactor) obligatoria para accesos privilegiados; revisión periódica de privilegios de acceso; revocación inmediata de todos los accesos en caso de terminación de la relación laboral o contractual.
- Gestión de vulnerabilidades: pruebas de penetración y análisis de vulnerabilidades periódicos (mínimo anuales); parcheo de vulnerabilidades críticas en plazos definidos; proceso documentado de gestión de vulnerabilidades.
- Monitoreo y detección: monitoreo continuo de sistemas y redes; logs de auditoría conservados per la Política de Retención de Datos; detección y respuesta a anomalías; alertas en tiempo real para eventos críticos de seguridad.

3. TECHNICAL SECURITY CONTROLS (TOMs)

- Encryption: data in transit protected with TLS 1.2 or higher; data at rest encrypted with AES-256 or equivalent.
- Access control: RBAC (Role-Based Access Control); MFA mandatory for privileged access; periodic access privilege review; immediate revocation of all access upon termination of employment or contractual relationship.
- Vulnerability management: periodic penetration testing and vulnerability assessments (minimum annually); critical vulnerability patching within defined timeframes; documented vulnerability management process.
- Monitoring and detection: continuous systems and network monitoring; audit logs retained per Data Retention Policy; anomaly detection and response; real-time alerts for critical security events.

• Gestión de endpoints: protección de dispositivos finales; política de uso aceptable de dispositivos; gestión remota y borrado de dispositivos perdidos o robados.	• Endpoint management: end-device protection; device acceptable use policy; remote management and wiping of lost or stolen devices.
• Seguridad de la cadena de suministro: evaluación de seguridad de subencargados y proveedores críticos antes de la contratación; contratos con obligaciones de seguridad equivalentes per LPD y RGPD Art. 28(4).	• Supply chain security: security assessment of sub-processors and critical providers before engagement; contracts with equivalent security obligations per LPD and GDPR Art. 28(4).

4. FORMACIÓN, GESTIÓN DE INCIDENTES Y CONTINUIDAD

Formación y concienciación: formación obligatoria en seguridad de la información y protección de datos para todo el personal, con frecuencia mínima anual, actualizada ante cambios regulatorios significativos o nuevas amenazas relevantes. Se mantendrán registros de la formación impartida y de la asistencia del personal. Este procedimiento es coherente y debe leerse conjuntamente con la Política de Respuesta a Incidentes. En caso de Brecha de Datos Personales, se aplicará el procedimiento de notificación per LPD Art. 25: notificación a la ACE (Agencia de Ciberseguridad del Estado), Fiscalía General de la República y titulares afectados dentro de las 72 horas desde conocimiento razonable de la brecha, con posibilidad de notificaciones complementarias por fases cuando no sea posible proporcionar toda la información inicialmente. Los indicadores de rendimiento de seguridad (KPIs), incluyendo tiempos de respuesta a incidentes, plazos de parcheo y tasa de resolución de vulnerabilidades, serán monitoreados y reportados periódicamente al Director.

4. TRAINING, INCIDENT MANAGEMENT AND CONTINUITY

Training and awareness: mandatory information security and data protection training for all staff, at minimum annually, updated upon significant regulatory changes or new relevant threats. Records of training delivered and staff attendance shall be maintained. This procedure is coherent and should be read in conjunction with the Incident Response Policy. In case of Personal Data Breach, the LPD Art. 25 notification procedure applies: notification to ACE (Agencia de Ciberseguridad del Estado), Fiscalía General de la República and affected data subjects within 72 hours of reasonable knowledge of the breach, with possibility of supplementary phased notifications where not all information can be provided initially. Security performance indicators (KPIs), including incident response times, patching timelines and vulnerability resolution rates, are monitored and reported periodically to the Director.

5. CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN ANTE DESASTRES

Cryptadium mantiene BCP y DRP documentados, probados periódicamente y actualizados para garantizar la continuidad del servicio de procesamiento de pagos en Bitcoin ante interrupciones graves. Los planes definen: RTO y RPO acordes con el SLA vigente; procedimientos de activación y escalada; responsabilidades del personal clave;

5. BUSINESS CONTINUITY AND DISASTER RECOVERY

Cryptadium maintains documented, periodically tested and updated BCP and DRP to ensure Bitcoin payment processing service continuity in the event of severe disruptions. Plans define: RTO and RPO consistent with the applicable SLA; activation and escalation procedures; key personnel responsibilities; and communication with

y comunicación con Comerciantes y autoridades. Los planes se prueban mínimo una vez al año. El acceso a la información sobre los BCP/DRP se limita conforme al principio de mínimo privilegio y necesidad de conocer.	Merchants and authorities. Plans are tested at minimum annually. Access to BCP/DRP information is limited per least privilege and need-to-know principles.
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. | security@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. | security@cryptadium.com*

© 2026 DUALPAY, S.A. de C.V. (CRYPTADIUM). Todos los derechos reservados / All rights reserved.