CRYPTADIUM

POLÍTICA DE RESPUESTA A INCIDENTES

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 Respuesta a Incidentes establece los procedimientos de DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.), operando como CRYPTADIUM, para la detección, contención, notificación, remediación y revisión post-incidente de los incidentes de seguridad, incluyendo brechas de datos personales, incidentes AML/CFT/FP, y fallos operativos materiales en el servicio de procesamiento de pagos en Bitcoin, conforme a la LPD (DL 144/2024), LEPLAF (DL 426/2025), LBAD (DL 643/11 enero 2023) y obligaciones regulatorias CNAD/UIF/ACE/Fiscalía. Esta Política es coherente con la Política de Seguridad de la Información, el APD/DPA v4.0 y la Política de Privacidad v4.0. Se designará un Incident Response Lead responsable de la coordinación de cada incidente, toma de decisiones operativas y comunicación con autoridades y partes afectadas. Se mantendrá un registro centralizado de incidentes (Incident Log) con el historial, estado y resolución de todos los incidentes.

2. CLASIFICACIÓN DE INCIDENTES

CRYPTADIUM

INCIDENT RESPONSE 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 Incident Response Policy establishes the procedures of DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.), operating as CRYPTADIUM, for the detection, containment, notification, remediation and post-incident review of security incidents, including personal data breaches, AML/CFT/PF incidents and material operational failures in the Bitcoin payment processing service, pursuant to LPD (DL 144/2024), LEPLAF (DL 426/2025), LBAD (DL 643/11 January 2023) and CNAD/UIF/ACE/Fiscalía regulatory obligations. This Policy is coherent with the Information Security Policy, DPA v4.0 and Privacy Policy v4.0. An Incident Response Lead shall be designated, responsible for incident coordination, operational decision-making and communication with authorities and affected parties. A centralised Incident Log shall be maintained with the history, status and resolution of all incidents.

2. INCIDENT CLASSIFICATION

• Nivel 1 — Crítico: incidente con impacto material en la seguridad de datos personales, capacidad de procesamiento de Transacciones en Bitcoin, cumplimiento AML/CFT/FP, o que requiere notificación regulatoria inmediata. Tiempo de primera respuesta: 1 hora. Escalada inmediata al Director, MLRO e Incident Response Lead.	• Level 1 — Critical: incident with material impact on personal data security, Bitcoin Transaction processing capacity, AML/CFT/PF compliance, or requiring immediate regulatory notification. First response time: 1 hour. Immediate escalation to Director, MLRO and Incident Response Lead.
• Nivel 2 — Alto: incidente con impacto significativo pero controlable, sin notificación regulatoria inmediata requerida. Tiempo de primera respuesta: 4 horas.	• Level 2 — High: incident with significant but controllable impact, no immediate regulatory notification required. First response time: 4 hours.
• Nivel 3 — Medio: incidente con impacto limitado, sin afectación a datos personales ni a la continuidad del servicio. Tiempo de primera respuesta: 1 Día Hábil.	• Level 3 — Medium: incident with limited impact, no effect on personal data or service continuity. First response time: 1 Business Day.
• Nivel 4 — Bajo: incidente menor, sin impacto en datos personales ni continuidad del servicio. Gestión rutinaria dentro de 3 Días Hábiles.	• Level 4 — Low: minor incident, no impact on personal data or service continuity. Routine management within 3 Business Days.

3. PROCEDIMIENTO DE RESPUESTA A INCIDENTES

3. INCIDENT RESPONSE PROCEDURE

Fase 1: Detección e Identificación	**Phase 1: Detection and Identification**
Cualquier empleado, sistema automatizado o proveedor externo que detecte o sospeche de un incidente reportará inmediatamente a incidents@cryptadium.com y al MLRO cuando el incidente pueda tener implicaciones AML/CFT/FP. La documentación inicial incluirá: fecha/hora de detección, naturaleza del incidente, sistemas afectados, datos potencialmente comprometidos. El Incident Response Lead es notificado en todos los incidentes de Nivel 1 y Nivel 2. Todos los incidentes se registran en el Incident Log centralizado.	Any employee, automated system or external provider detecting or suspecting a security incident shall immediately report to incidents@cryptadium.com and to the MLRO where AML/CFT/PF implications may exist. Initial documentation shall include: detection date/time, nature of incident, affected systems, potentially compromised data. The Incident Response Lead is notified for all Level 1 and Level 2 incidents. All incidents are recorded in the centralised Incident Log.
Fase 2: Contención	**Phase 2: Containment**
El Incident Response Lead coordina las medidas de contención inmediata: aislamiento de sistemas afectados; bloqueo de accesos comprometidos; suspensión temporal de servicios afectados; y preservación de evidencias forenses. Ninguna medida de contención que implique retención de fondos Bitcoin de Comerciantes constituirá confiscación ni transferencia de propiedad sin orden de autoridad competente.	The Incident Response Lead coordinates immediate containment measures: isolation of affected systems; blocking of compromised access; temporary suspension of affected services; and preservation of forensic evidence. No containment measure involving retention of Merchant Bitcoin funds shall constitute confiscation or transfer of ownership without an order from a competent authority.

Fase 3: Notificación a Autoridades (Plazos Críticos)	Phase 3: Notification to Authorities (Critical Deadlines)
Brecha de datos personales per LPD Art. 25 — MÁXIMO 72 HORAS desde conocimiento razonable de la brecha: notificación a ACE (Agencia de Ciberseguridad del Estado) + Fiscalía General de la República + titulares afectados. Cuando Cryptadium actúe como encargado del tratamiento: MÁXIMO 48 HORAS → notificación al Comerciante (Responsable) para que éste cumpla su obligación de 72 horas. Notificaciones complementarias por fases cuando no sea posible proporcionar toda la información inicialmente. El Incident Response Lead coordina todas las comunicaciones con autoridades. Las comunicaciones externas (incluyendo comunicados a Comerciantes, socios y, cuando aplique, divulgaciones públicas) serán coordinadas y aprobadas por el Director o la autoridad designada antes de su emisión.	**Personal data breach per LPD Art. 25 — MAXIMUM 72 HOURS from reasonable knowledge of the breach: notification to ACE + Fiscalía General de la República + affected data subjects. When Cryptadium acts as data processor: MAXIMUM 48 HOURS → notification to the Merchant (Controller) so it can fulfil its 72-hour obligation. Supplementary phased notifications where not all information can be provided initially. The Incident Response Lead coordinates all communications with authorities. External communications (including to Merchants, partners and, where applicable, public disclosures) shall be coordinated and approved by the Director or designated authority before issuance.**
Fase 4: Erradicación y Recuperación	**Phase 4: Eradication and Recovery**
Bajo la coordinación del Incident Response Lead: identificación y eliminación de la causa raíz; restauración de sistemas desde backups verificados; verificación de la integridad de los datos restaurados; y reanudación gradual y controlada del servicio de procesamiento de pagos en Bitcoin.	Under the Incident Response Lead's coordination: identification and elimination of the root cause; system restoration from verified backups; verification of restored data integrity; and gradual, controlled resumption of Bitcoin payment processing services.
Fase 5: Revisión Post-Incidente	**Phase 5: Post-Incident Review**
Dentro de los 30 días siguientes a la resolución del incidente: análisis de causa raíz documentado; evaluación del impacto real; revisión de la efectividad de los controles aplicados; identificación de mejoras; y actualización de políticas, procedimientos y controles técnicos. El Incident Response Lead elaborará un informe post-incidente aprobado por el Director antes de su archivo. El Incident Log se actualiza con la resolución final del incidente.	Within 30 days of incident resolution: documented root cause analysis; actual impact assessment; effectiveness review of applied controls; improvement identification; and update of policies, procedures and technical controls. The Incident Response Lead shall prepare a post-incident report approved by the Director before filing. The Incident Log is updated with the final incident resolution.
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. | incidents@cryptadium.com | 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. | incidents@cryptadium.com | security@cryptadium.com*