# CRYPTADIUM

## POLÍTICA DE DIVULGACIÓN DE VULNERABILIDADES

*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. COMPROMISO DE CRYPTADIUM CON LA SEGURIDAD

DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.), operando como CRYPTADIUM, valora las contribuciones de la comunidad de seguridad en la identificación responsable de vulnerabilidades en nuestros sistemas. Esta Política de Divulgación de Vulnerabilidades (VDP) establece el marco para que investigadores de seguridad y cualquier persona que descubra una vulnerabilidad potencial en los sistemas de Cryptadium puedan comunicarla de forma responsable, contribuyendo a la seguridad del servicio de procesamiento de pagos en Bitcoin y a la protección de los datos personales tratados por Cryptadium per la LPD (DL 144/2024), la LEPLAF (DL 426/2025) y las obligaciones de seguridad de la CNAD y la ACE (Agencia de Ciberseguridad del Estado). Esta Política es coherente con la Política de Seguridad de la Información y la Política de Respuesta a Incidentes de Cryptadium.

### 2. ÁMBITO DE LA VDP

# CRYPTADIUM

## VULNERABILITY DISCLOSURE 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. CRYPTADIUM'S SECURITY COMMITMENT

DUALPAY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (DUALPAY, S.A. de C.V.), operating as CRYPTADIUM, values the security community's contributions in the responsible identification of vulnerabilities in our systems. This Vulnerability Disclosure Policy (VDP) establishes the framework for security researchers and anyone discovering a potential vulnerability in Cryptadium's systems to report it responsibly, contributing to the security of the Bitcoin payment processing service and the protection of personal data processed by Cryptadium per LPD (DL 144/2024), LEPLAF (DL 426/2025) and CNAD and ACE (Agencia de Ciberseguridad del Estado) security obligations. This Policy is coherent with Cryptadium's Information Security Policy and Incident Response Policy.

### 2. VDP SCOPE

### 2.1 En Alcance

- API de procesamiento de pagos en Bitcoin de Cryptadium (endpoints de producción y sandbox documentados en cryptadium.com/developers).
- Portal del Comerciante (cryptadium.com/portal).
- Sitio web principal de Cryptadium (cryptadium.com).

### 2.2 Fuera de Alcance

- Sistemas de terceros proveedores o clientes de Cryptadium no gestionados directamente por Cryptadium.
- Ataques de denegación de servicio (DoS/DDoS), pruebas de fuerza bruta, spam, ingeniería social o phishing.
- Pruebas realizadas en cuentas de otros usuarios o Comerciantes sin su consentimiento expreso.
- Vulnerabilidades en software de terceros no modificado por Cryptadium (a menos que demuestren impacto directo en los sistemas de Cryptadium).

### 2.1 In Scope

- Cryptadium Bitcoin payment processing API (production and sandbox endpoints documented at cryptadium.com/developers).
- Merchant Portal (cryptadium.com/portal).
- Cryptadium main website (cryptadium.com).

### 2.2 Out of Scope

- Third-party providers' or clients' systems not directly managed by Cryptadium.
- Denial of service attacks (DoS/DDoS), brute force testing, spam, social engineering or phishing.
- Tests conducted on other users' or Merchants' accounts without their express consent.
- Vulnerabilities in unmodified third-party software (unless demonstrating direct impact on Cryptadium systems).

## 3. PROCESO DE REPORTE RESPONSABLE

Para reportar una vulnerabilidad de seguridad de forma responsable: (1) envía tu reporte a security@cryptadium.com con el asunto "[VDP] Informe de Vulnerabilidad"; (2) incluye en el reporte: descripción de la vulnerabilidad, sistemas afectados, pasos para reproducirla, impacto potencial estimado y prueba de concepto (sin causar daño real ni acceder a datos reales de terceros); (3) no divulgues públicamente la vulnerabilidad hasta que Cryptadium haya confirmado la resolución o hayan transcurrido 90 días desde el reporte original; Cryptadium podrá solicitar períodos de no divulgación extendidos cuando sea necesario por razones de seguridad o regulatorias, incluyendo requisitos de

## 3. RESPONSIBLE REPORTING PROCESS

To report a security vulnerability responsibly: (1) send your report to security@cryptadium.com with the subject "[VDP] Vulnerability Report"; (2) include in the report: vulnerability description, affected systems, reproduction steps, estimated potential impact and proof of concept (without causing actual harm or accessing real third-party data); (3) do not publicly disclose the vulnerability until Cryptadium has confirmed resolution or 90 days have passed since the original report; Cryptadium may request extended non-disclosure periods where necessary for security or regulatory reasons, including CNAD or ACE requirements; and (4) do not access, modify, delete,

la CNAD o la ACE; y (4) no accedas, modifiques, elimines, copies ni exfiltres datos de otros usuarios, Comerciantes o de Cryptadium durante la investigación.

> *La investigación de seguridad que implique acceso no autorizado a datos personales puede constituir una brecha de datos per la LPD (DL 144/2024) y deberá ser notificada a Cryptadium de inmediato. Cryptadium actuará conforme a sus obligaciones de notificación per LPD Art. 25 si la brecha así lo requiere.*

copy or exfiltrate data belonging to other users, Merchants or Cryptadium during the investigation.

> *Security research involving unauthorised access to personal data may constitute a data breach under LPD (DL 144/2024) and must be immediately notified to Cryptadium. Cryptadium will act in accordance with its notification obligations under LPD Art. 25 if the breach so requires.*

## 4. COMPROMISOS DE CRYPTADIUM Y LIMITACIONES

Cryptadium se compromete a: (a) acusar recibo del reporte dentro de las 5 horas hábiles siguientes a su recepción; (b) investigar la vulnerabilidad reportada de buena fe y en coordinación con el Incident Response Lead designado; (c) mantener comunicación con el investigador durante el proceso de investigación y remediación; y (d) notificar al investigador cuando la vulnerabilidad haya sido remediada. Cryptadium NO ofrece recompensas económicas (bug bounty) per esta VDP salvo que se indique expresamente en un programa de bug bounty separado publicado en cryptadium.com/security. Esta VDP no es una autorización para realizar pruebas de penetración no solicitadas ni constituye una exención de responsabilidad legal por accesos no autorizados a sistemas de Cryptadium. Los investigadores que actúen de buena fe conforme a esta VDP no serán objeto de acciones legales por parte de Cryptadium, siempre que respeten el ámbito y los límites definidos en la Sección 3. Las vulnerabilidades podrán ser clasificadas por severidad (Baja, Media, Alta, Crítica), lo que podrá afectar la priorización y los plazos de respuesta y remediación.

*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*

## 4. CRYPTADIUM'S COMMITMENTS AND LIMITATIONS

Cryptadium commits to: (a) acknowledging receipt of the report within 5 business hours of receipt; (b) investigating the reported vulnerability in good faith and in coordination with the designated Incident Response Lead; (c) maintaining communication with the researcher during the investigation and remediation process; and (d) notifying the researcher when the vulnerability has been remediated. Cryptadium does NOT offer financial rewards (bug bounty) under this VDP unless expressly stated in a separate bug bounty programme published at cryptadium.com/security. This VDP is not an authorisation to conduct unsolicited penetration testing and does not constitute a legal exemption for unauthorised access to Cryptadium systems. Researchers acting in good faith per this VDP will not be subject to legal action by Cryptadium, provided they respect the scope and limits defined in Section 3. Vulnerabilities may be classified by severity (Low, Medium, High, Critical), which may affect prioritisation and response and remediation timelines.

*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*