POLÍTICA PÚBLICA – SECURITY DISCLOSURE / VULNERABILITY REPORTING POLICY

Reporte responsable de vulnerabilidades y hallazgos de seguridad

CripCom (App / Web)

vs.001 – SELLADO

Entidad: CripCom Trade LLC (USA)
Fecha: 07-Mar-2026

ESTADO	SELLADO (vs.001) - Documento público
VERSIÓN	vs.001
FECHA	07-Mar-2026
OWNER / RESPONSABLE DOCUMENTAL	LDO (LEGAL DOCUMENT OFFICER)
APROBADOR (SPONSOR)	CLO (CHIEF LEGAL OFFICER)
OBJETIVO	Establecer el marco público para el reporte responsable de vulnerabilidades y hallazgos de seguridad, sin autorizar pruebas intrusivas ni crear obligaciones de recompensa.
DOCUMENTOS RELACIONADOS	TyC Plataforma + Anexos | Política de Canales Oficiales | Política de Privacidad | Disclaimer | Política de PQRS.

1. Principio

CripCom puede poner a disposición un canal o mecanismo oficial para que terceros reporten, de buena fe, vulnerabilidades, fallas técnicas o hallazgos de seguridad que puedan afectar razonablemente la App, la web o servicios relacionados. Esta Política busca promover divulgación responsable, reducir riesgos innecesarios y ordenar expectativas sobre el tratamiento de dichos reportes.

2. Alcance

Esta Política aplica a reportes de seguridad relacionados con activos digitales, aplicaciones, flujos web, APIs, componentes visibles públicamente, configuraciones expuestas o comportamientos técnicos que, de manera razonable, puedan generar riesgos de confidencialidad, integridad, disponibilidad o uso no autorizado.

La aplicabilidad concreta dependerá del entorno, del servicio y de la información disponible al momento del reporte.

3. Qué tipo de hallazgos pueden ser reportados

De manera orientativa, un reporte puede incluir, entre otros, hallazgos como:

- exposición no intencional de información sensible o acceso indebido a datos;
- errores de autenticación, autorización o control de acceso;
- fallas que permitan escalamiento indebido de privilegios, ejecución no autorizada o bypass de controles;
- configuraciones inseguras, endpoints expuestos o comportamientos anómalos con impacto razonable de seguridad;
- riesgos técnicos que puedan afectar disponibilidad o integridad de sistemas o flujos críticos.

4. Qué NO está permitido

Esta Política no autoriza pruebas intrusivas, explotación activa ni conductas que puedan afectar usuarios, terceros, infraestructura o continuidad operativa. En particular, no está permitido:

- acceder, modificar, extraer, descargar, publicar o conservar datos personales o información de terceros más allá de lo estrictamente necesario para describir el hallazgo;
- realizar ataques de denegación de servicio, spam, fuerza bruta, malware, ingeniería social, phishing o cualquier técnica disruptiva;
- persistir en sistemas, crear cuentas ficticias masivas, encadenar explotación o intentar monetizar el hallazgo;
- afectar cuentas reales, credenciales, pagos, activos, integraciones o proveedores;
- divulgar públicamente un hallazgo antes de permitir a CripCom un tiempo razonable para evaluarlo y gestionarlo.

5. Cómo reportar de manera responsable

El reporte deberá realizarse exclusivamente a través de los canales oficiales publicados por CripCom. En la medida de lo posible, quien reporta debería incluir:

- descripción clara del hallazgo;
- fecha de detección y entorno observado;
- pasos razonables para reproducir el comportamiento, sin incluir instrucciones innecesariamente peligrosas;
- evidencia mínima suficiente, como capturas, logs o referencias técnicas pertinentes;
- datos de contacto para seguimiento, si quien reporta desea recibir respuesta.

6. Qué puede esperar quien reporta

CripCom procurará revisar los reportes recibidos de buena fe, priorizarlos conforme a su criticidad aparente y, cuando resulte apropiado, acusar recibo o solicitar información adicional. Los tiempos de revisión, respuesta o corrección pueden variar según la complejidad del caso, disponibilidad operativa, dependencia de terceros y riesgo asociado.

7. Sin recompensa automática ni autorización implícita

Esta Política no constituye una invitación general a probar sistemas, no crea una relación contractual con quien reporta y no establece obligación de compensación, reconocimiento público, pago, bounty, safe harbor irrestricto ni plazo fijo de respuesta. Cualquier reconocimiento o interacción quedará a la exclusiva discreción de CripCom y sujeto a ley aplicable, evidencia disponible y conducta observada.

8. Privacidad, confidencialidad y tratamiento del reporte

CripCom podrá tratar la información recibida en un reporte de seguridad para fines de validación, gestión de incidentes, mejora de controles, coordinación con proveedores, cumplimiento legal y defensa de derechos. Quien reporta no debe incluir datos innecesarios de terceros. El tratamiento de información personal se regirá por la Política de Privacidad vigente y por las limitaciones legales aplicables.

9. Coordinación con terceros y limitaciones

Algunos hallazgos pueden involucrar servicios de terceros, infraestructura externa o componentes fuera del control directo de CripCom. En tales casos, CripCom podrá remitir, coordinar o escalar el asunto según corresponda, sin asumir control integral sobre los tiempos, decisiones o medidas adoptadas por dichos terceros.

10. Cambios y control de versión

Esta Política puede actualizarse. La versión vigente será la publicada en los canales oficiales. Cambios materiales podrán reflejarse en una nueva versión sellada o en la actualización correspondiente dentro de la biblioteca legal pública de CripCom.