ANEXO PP-E — RESUMEN DE SEGURIDAD Y RESPUESTA A INCIDENTES CRIPCOM (APP / WEB)
vs.001 — SELLADO

Entidad responsable: CripCom Trade LLC (USA)
Fecha: 06-Mar-2026

ESTADO	SELLADO (v.001) — ANEXO PP-E
VERSIÓN	vs.001
FECHA	06-Mar-2026
OWNER / RESPONSABLE	LDO (LEGAL DOCUMENT OFFICER)
APROBADOR (SPONSOR)	CLO (CHIEF LEGAL OFFICER)
DOCUMENTO MADRE	Política de Privacidad CripCom Trade LLC — ES vs.001 / EN vs.001
OBJETIVO	Describir, a alto nivel, el enfoque de seguridad y respuesta a incidentes sin exponer información sensible.

E1. Principio

CripCom aplica controles técnicos y organizativos razonables para proteger datos personales. Este anexo es un resumen público de alto nivel; no detalla configuraciones internas ni superficies de ataque.

E2. Controles de seguridad (alto nivel)

- CripCom aplica, a nivel general, controles de seguridad razonables y proporcionales a la naturaleza de sus operaciones y de los datos tratados. Estos controles pueden incluir, entre otros:
  a. **Controles de acceso**, bajo criterios de mínimo privilegio y segregación de funciones.
  b. **Medidas de protección de la información**, incluyendo resguardos para datos en tránsito y, cuando corresponda, en reposo.
  c. **Monitoreo y registros**, con fines de detección de anomalías, investigación y trazabilidad operativa.

d. **Gestión de proveedores**, priorizando terceros que mantengan estándares razonables de seguridad para los servicios que soportan la operación.
e. **Continuidad y resiliencia operativa**, incluyendo respaldos, recuperación y medidas de respuesta según políticas internas aplicables.

E3. Gestión de incidentes

Ante un incidente, CripCom puede:

a. Investigar y contener el incidente (aislar sistemas, revocar accesos, aplicar mitigaciones).
b. Activar medidas de protección adicionales (verificaciones extra, bloqueos temporales por seguridad).
c. Preservar evidencia técnica para análisis y auditoría (logs, timestamps, eventos).

E4. Notificación

Cuando corresponda conforme a la ley aplicable, CripCom notificará a usuarios y/o autoridades dentro de los plazos requeridos. La notificación puede realizarse por email, in-app o canales oficiales, según el alcance del incidente.

E5. Responsabilidad del usuario

El usuario contribuye a la seguridad cuando:

a. Protege su dispositivo y credenciales.
b. Evita compartir códigos de autenticación.
c. Usa solo canales oficiales para soporte y comunicaciones.

E6. Limitaciones

Ningún sistema es 100% seguro. Aunque CripCom aplica medidas razonables, no puede garantizar seguridad absoluta. Este anexo no sustituye obligaciones legales ni compromisos contractuales específicos con proveedores.

E7. Registro de cambios

Fecha	Cambio	Motivo	Aprobador
06-Mar-2026	Creación v.001	Resumen público de seguridad/IR	CLO (CHIEF LEGAL OFFICER)