

El Incidente Bithumb: Un Caso de Estudio en Riesgo Operacional

Anatomía de un error de 35.700 millones de euros y el fracaso de los controles internos



Resumen Ejecutivo: La fragilidad de la automatización sin control



EL EVENTO

Durante una campaña promocional, **Bithumb** transfirió por error **620.000 BTC** a **249 usuarios** debido a un error de entrada de datos ('BTC' vs. 'KRW').



EL IMPACTO

Una exposición potencial de ~USD 42.840 millones. Aunque se recuperó el 99,7%, la pérdida neta final fue de USD 12,85 millones.



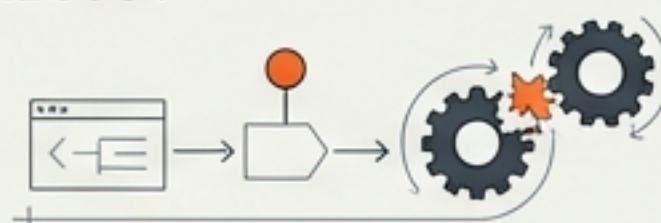
LA CAUSA RAÍZ

No fue un ciberataque, sino un fallo operativo interno caracterizado por la ausencia de **validación automática**, **límites transaccionales** y **segregación de funciones (SoD)**.



LA LECCIÓN

El incidente subraya que la **automatización sin gobernanza amplifica el error humano** a niveles sistémicos.



Contexto del Incidente: El error de tecleo más costoso de la historia



EL GATILLADOR

Un error humano simple en la parametrización de una variable crítica (Tipo de Activo).

EL RESULTADO

249 usuarios recibieron criptoactivos reales en lugar de créditos promocionales.

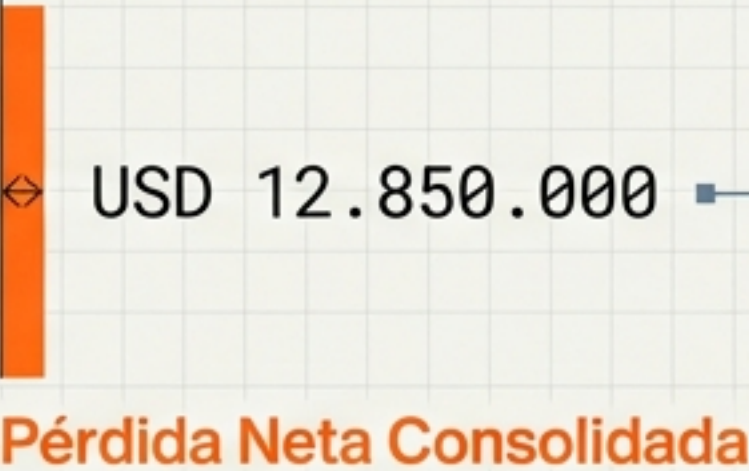
DATO CLAVE

No fue un hackeo externo. Fue un colapso de los controles internos.

Forensic editorial slide

Análisis de Impacto: Exposición Potencial vs. Pérdida Real

Exposición Potencial



LA RECUPERACIÓN

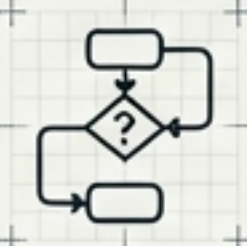
Tasa de Recuperación: 99,7%.

Sin embargo, el 0,3% restante representa una pérdida millonaria directa, sin contar los costos reputacionales y legales.

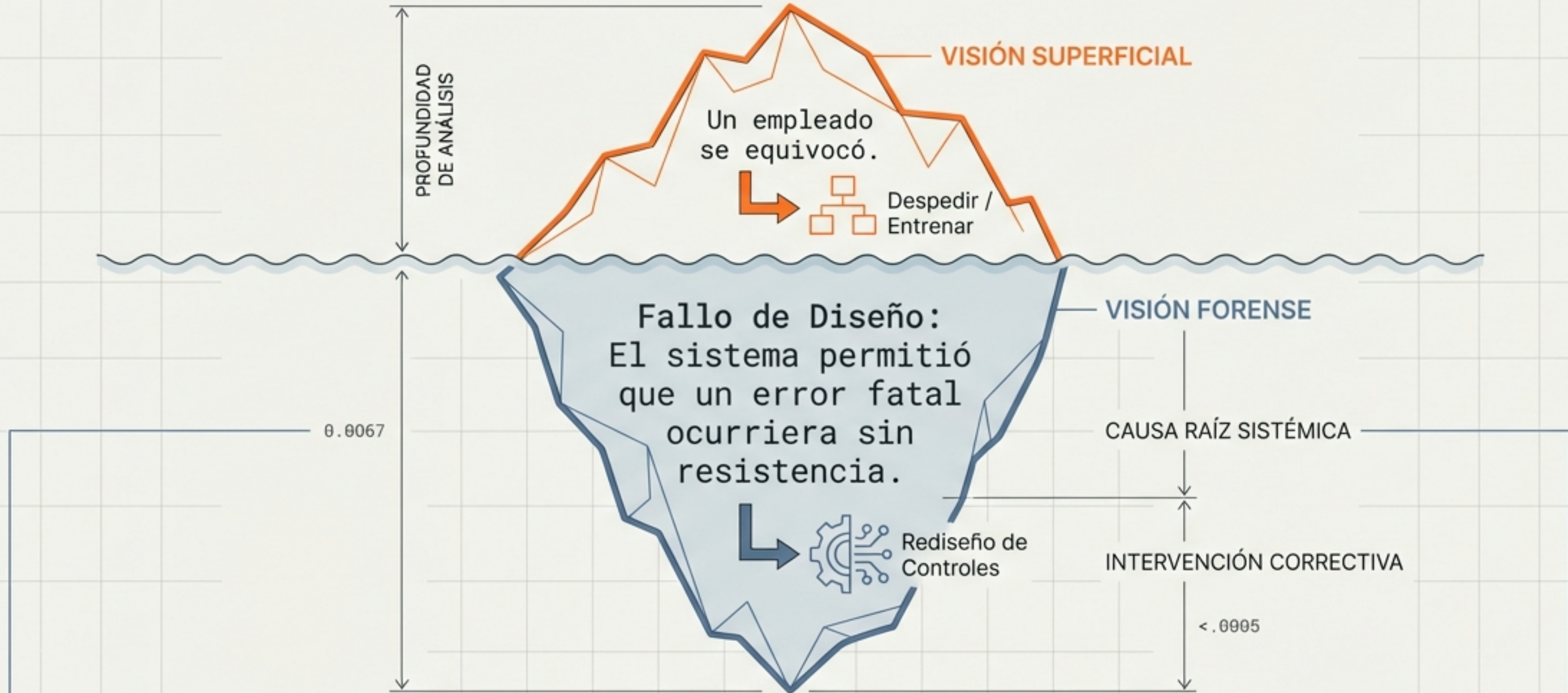
Insight: Aunque la recuperación fue alta, el riesgo inherente materializado fue de escala macroeconómica.

Clasificación del Riesgo (Marco Basel / ISO 31000)



TIPO DE EVENTO	Error de procesamiento y ejecución / Fallo en gestión de procesos.		
CAUSA RAÍZ	Factor humano + Deficiencia en controles preventivos + Fallo en diseño de sistemas.		
EVALUACIÓN DE RIESGO INHERENTE	1. 	Probabilidad: MEDIA (Procesos Manuales)	2.  Impacto Financiero: EXTREMO
	3. 	Impacto Regulatorio: MUY ALTO	4.  Impacto Sistémico: CRÍTICO

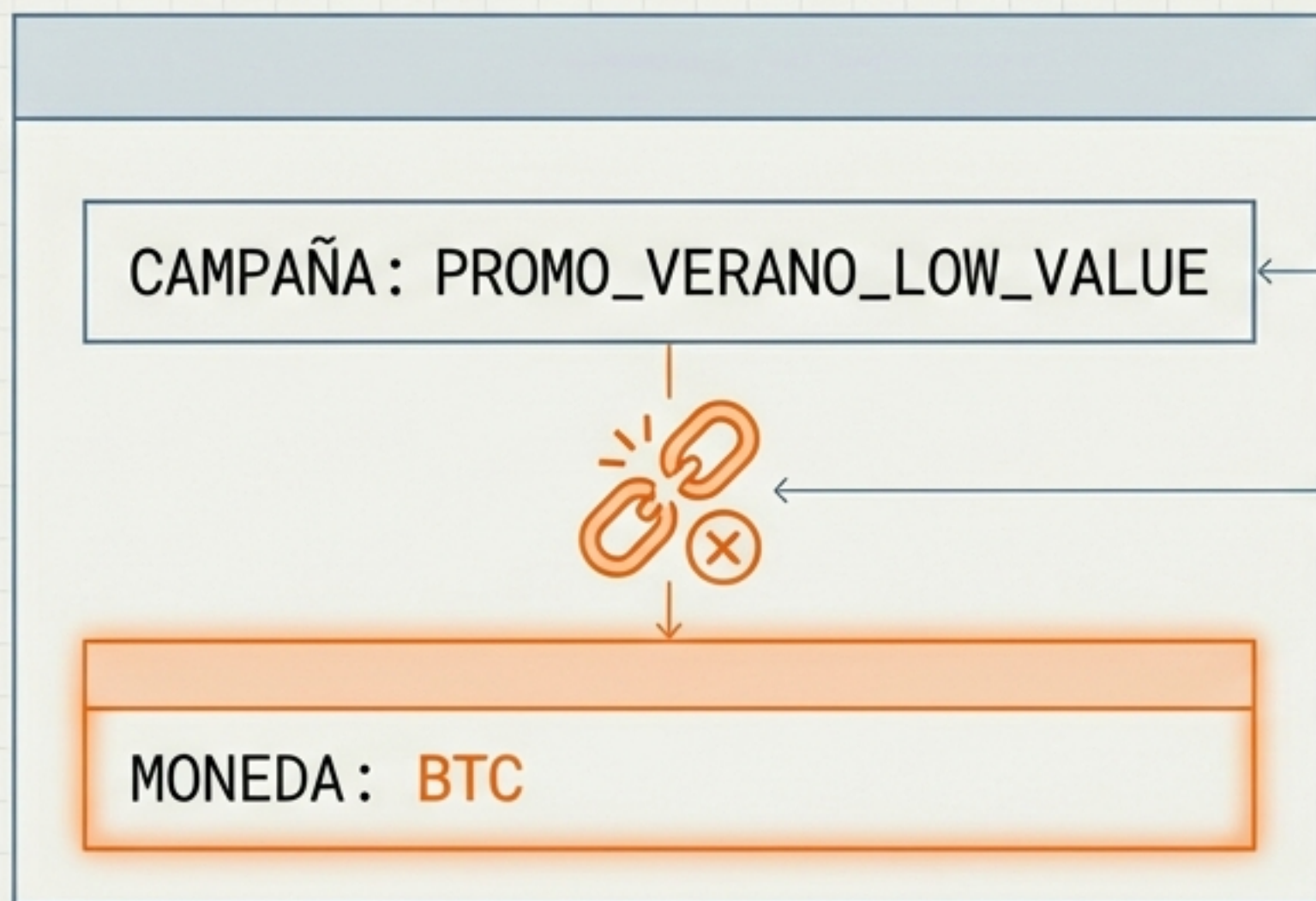
El mito del “Error Humano”



“Un sistema robusto debe asumir que el error humano ocurrirá y debe estar diseñado para contenerlo, no para amplificarlo.”

Falla de Control #1: Validación de Entradas (Input Validation)

**ESTADO:
INEXISTENTE**



EL FALLO

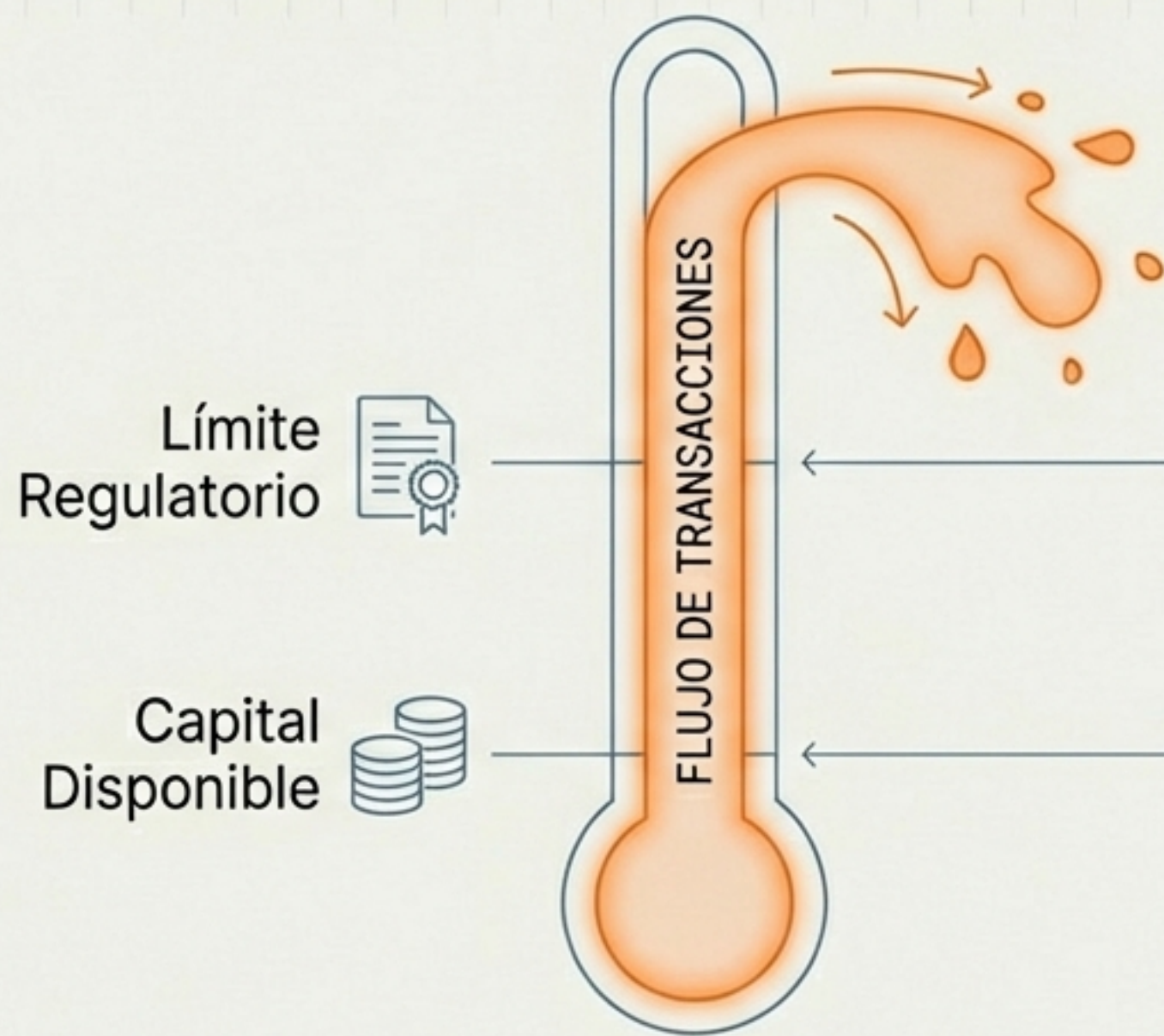
El sistema aceptó 'BTC' en un campo destinado a una promoción de bajo valor sin verificar la coherencia lógica.

LO QUE DEBIÓ OCURRIR (VALIDACIÓN CRUZADA)

- [•] Comparación automática: [Tipo de Activo] vs. [Tipo de Campaña].
- [•] Hard Stop: Bloqueo técnico ante inconsistencias de tipo de dato.

Falla de Control #2: Ausencia de Límites Transaccionales

**ESTADO:
CRÍTICO**



EL FALLO

Se permitieron transferencias masivas que superaban los umbrales de capital regulatorio sin ningún bloqueo sistémico.

LO QUE DEBIÓ OCURRIR (CONTROLES REQUERIDOS)

- [X] **Hard Stop por Monto Máximo:** Límites duros que impiden la ejecución técnica.
- [X] **Umbrales de Exposición:** Validación contra el capital disponible.
- [X] **Aprobación Multinivel:** Requisito obligatorio para pagos extraordinarios.

Falla de Control #3: Segregación de Funciones (SoD)

**ESTADO:
VULNERABLE**

Violación de principios COSO 2013



LA SOLUCIÓN:

Separación estricta entre quien DISEÑA la campaña (Marketing) y quien AUTORIZA el pago (Tesorería).

CONCENTRACIÓN DE RIESGO

Falla de Gobernanza: El Principio de los “Cuatro Ojos”

**ESTADO:
CRÍTICO**

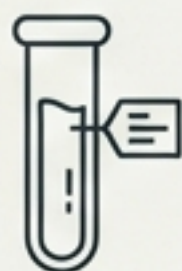


**La falta de este flujo convirtió un error individual
en una crisis corporativa.**

Déficit en la Gobernanza de Procesos

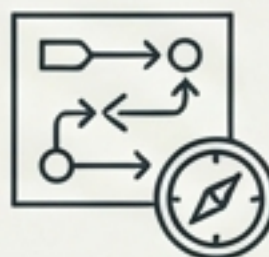
PREGUNTA CLAVE: ¿Se realizó un análisis de riesgo antes de lanzar la campaña?

NO



FALTA DE TESTING

Ausencia de pruebas en ambiente sandbox para verificar los parámetros de pago.



PROCESOS INFORMALES

Inexistencia de un mapa de procesos (BPM) formal con roles RACI definidos.



GESTIÓN DE CAMBIOS

Falta de protocolos para la modificación de variables críticas en producción.

Gestión de Crisis: Respuesta y Consecuencias

ACIERTOS (Respuesta Inmediata)



Suspensión de transacciones.



Comunicación pública rápida.



Coordinación con reguladores.

**RESULTADO: 99,7% de
fondos recuperados.**



ERRORES (Riesgos Derivados)



Congelamiento masivo de cuentas.



Riesgo Legal significativo
(Demandas de usuarios).



Riesgo Regulatorio
(Intervención de la Comisión).



**RIESGOS CRÍTICOS
IDENTIFICADOS: ALTO IMPACTO
REGULATORIO Y LEGAL**

El Blueprint: Marco de Control Robusto



Tablero de Control: Indicadores Clave de Riesgo (KRIs)



"Lo que no se mide, no se controla."

SCALE →

Reflexión Final: Cultura sobre Cumplimiento



**GOBERNANZA
ROBUSTA**



**CONTROLES
AUTOMÁTICOS**



**CULTURA
DE RIESGO**



= SEGURIDAD

- Decir que "no hubo un fallo de seguridad" es técnicamente correcto pero irrelevante. Hubo un colapso del Gobierno Corporativo.
- En entornos de activos digitales, el riesgo operacional escala a sistémico en minutos.

**LA AUTOMATIZACIÓN SIN CONTROL NO ES EFICIENCIA;
ES AMPLIFICACIÓN DEL ERROR.**