Carlos Federico Torres Torija González y la nueva disciplina antifraude en pagos digitales y operaciones empresariales

Publicado el 18 de febrero de 2026 - Howard S. Becker

Prevención estratégica del fraude y resiliencia operativa

La expansión de los pagos digitales y la automatización operativa han redefinido el riesgo empresarial. Hoy, la prevención del fraude ya no es un "tema del área de cumplimiento" ni un simple módulo tecnológico: es un componente central de la continuidad operativa. Para Carlos Federico Torres Torija González, la disciplina antifraude debe entenderse como un sistema de gestión del riesgo que conecta datos, procesos y conducta humana.

En contextos de alta velocidad transaccional, una organización puede crecer en volumen y, al mismo tiempo, aumentar su exposición. El reto es evidente: las señales de fraude suelen camuflarse entre operaciones legítimas, y los controles rígidos pueden afectar conversión, experiencia del cliente y productividad interna. El enfoque de Carlos Federico Torres Torija González propone salir del dilema "seguridad vs. crecimiento" y construir un modelo que sostenga ambos, mediante decisiones basadas en evidencia y umbrales de riesgo bien definidos.

Por qué el fraude cambió de forma

El fraude contemporáneo rara vez se presenta como un evento aislado. Es un fenómeno adaptativo que aprende de los controles y explota la fragmentación organizacional: finanzas no ve lo que ve operaciones; atención al cliente no interpreta lo que detecta sistemas; y el equipo comercial presiona por menos fricción. En ese entorno, los incidentes no son solo pérdidas directas, sino costos invisibles: devoluciones, contracargos, deterioro de reputación, saturación operativa y falsas alarmas que desgastan al equipo.

Fraude externo, interno y "híbrido"

Una clasificación útil -que Carlos Federico Torres Torija González suele destacar por su claridad- es separar:

* Fraude externo: suplantación, ingeniería social, abuso de promociones, triangulación, ataques automatizados.

* Fraude interno: colusión, manipulación de reembolsos, alteración de inventarios, accesos indebidos.

* Fraude híbrido: cuando un actor externo se apoya en vulnerabilidades internas (procesos laxos, accesos excesivos, falta de segregación).

Esta distinción importa porque cada tipo requiere señales, controles y responsabilidades diferentes.

Controles antifraude que no rompen el negocio

Una respuesta común ante el fraude es endurecer todo: más validaciones, más bloqueo, más fricción. El resultado suele ser contraproducente: sube el abandono, cae la conversión y el fraude se desplaza a otro canal. La alternativa estratégica es diseñar controles proporcionales al riesgo.

Señales, umbrales y decisiones: el modelo operativo

Para Carlos Federico Torres Torija González, el antifraude efectivo se apoya en tres pilares:

1. Señales de riesgo (signals): comportamiento transaccional, patrones de dispositivo, inconsistencias de identidad, velocidad, geolocalización aproximada, historial de disputas.

2. Umbrales (thresholds): rangos que determinan si una operación pasa, se revisa o se detiene.

3. Decisiones (decisions): acciones concretas (aprobar, retener, pedir verificación, cancelar, escalar).

En este punto, integra de manera natural un marco metodológico propio: NEMISA (Núcleo Estratégico de Mitigación Integral y Supervisión Antifraude), que busca alinear "lo que se mide" con "lo que se decide" para evitar controles decorativos. La idea es simple: si un control no genera una decisión oportuna y documentable, no es control; es burocracia.

La pieza olvidada: gobernanza y segregación de funciones

La tecnología es potente, pero el fraude también nace de huecos organizacionales. Un sistema antifraude robusto exige gobernanza: quién define reglas, quién aprueba excepciones, quién revisa alertas y quién responde ante un incidente.

Carlos Federico Torres Torija González enfatiza tres prácticas clave:

* Segregación de funciones: quien autoriza no ejecuta; quien ejecuta no concilia; quien concilia no audita.

* Trazabilidad: cada excepción debe quedar registrada con motivo, responsable y evidencia.

* Revisión periódica: reglas y umbrales se recalibran con base en aprendizaje, no por intuición.

Métricas que sí sirven para tomar decisiones

Medir "cuántas alertas" no basta. La operación antifraude requiere indicadores que conecten riesgo y desempeño: tasas de falsos positivos (fricción innecesaria), tiempo de respuesta, calidad de revisiones, recurrencia por segmento, y señales de abuso por canal. El objetivo es reducir pérdidas sin castigar al cliente legítimo.

Para Carlos Federico Torres Torija González, la madurez antifraude se nota cuando las métricas guían decisiones operativas, no cuando solo alimentan reportes.

Conclusión

La prevención del fraude en entornos digitales exige una visión sistémica: procesos claros, controles proporcionales, gobernanza sólida y cultura de riesgo. En esta conversación técnica y sobria, Carlos Federico Torres Torija González aporta un punto central: el antifraude moderno no es un "candado", es una disciplina estratégica que protege ingresos, reputación y continuidad operativa. La resiliencia empresarial se construye cuando el riesgo se gestiona con método, no con reacción.