Nueva ley de fraude electrónico en Costa Rica: mayor responsabilidad para la banca

La Ley 10.889 redefine la protección del consumidor financiero en Costa Rica, obligando a los bancos a asumir la responsabilidad por fraudes electrónicos e introduciendo la inversión de la carga de la prueba, lo que exige a las entidades demostrar que cumplieron con los estándares de seguridad

Ficha rápida de la normativa

¿Qué es?
Ley que fortalece la protección del consumidor financiero en la custodia de su dinero frente a fraudes electrónicos.

¿A quién aplica?
Entidades financieras supervisadas: bancos, cooperativas y otros intermediarios.

¿Desde cuándo?
En vigor desde el 22 de abril de 2026.

¿Qué cambia con la ley 10.889?

La normativa introduce un cambio estructural en el sistema financiero:

- Se establece la responsabilidad objetiva de las entidades financieras ante fraudes, lo que implica que deben responder por la custodia de los fondos incluso sin culpa directa.
- El banco debe responder por operaciones no autorizadas realizadas por terceros, incluyendo casos de fraude electrónico y suplantación de identidad.
- Se introduce la inversión de la carga de la prueba, trasladando al banco la obligación de demostrar que actuó con la diligencia adecuada.

Claves regulatorias de la Ley 10.889

Inversión de la carga de la prueba y responsabilidad bancaria

Las entidades financieras responden por la sustracción de fondos bajo su custodia, incluso sin culpa directa. La ley introduce la inversión de la carga de la prueba en favor del consumidor: ante un fraude, es el banco quien debe demostrar que actuó con la diligencia adecuada y que el evento no fue atribuible a sus controles o procesos.

Gestión de reclamos y restitución

El proceso se formaliza con plazos y requisitos establecidos:

- 30 días para que el usuario presente el reclamo, el cual debe incluir una denuncia ante el Organismo de Investigación Judicial **(OIJ)**.
- 30 días para que la entidad resuelva, con una única prórroga posible en casos justificados.

Si el reclamo procede:

- Restitución de fondos en un máximo de 10 días, junto con la eliminación de cargos e intereses asociados.

Si la entidad incumple plazos:

- Se generan compensaciones automáticas para el usuario afectado.
- Si transcurren 120 días sin resolución, pierde la posibilidad de rechazar el reclamo.

Exigencias en ciberseguridad y control

Las entidades deben demostrar la implementación de controles adecuados en toda su operación:

- Monitoreo de patrones transaccionales y comportamiento habitual del usuario para detectar desviaciones.
- Identificación de dispositivos, canales, redes y hábitos de uso para validar consistencia operativa.
- Evaluación de consistencia operativa en cada interacción.

Las transacciones atípicas deben ser detectadas y confirmadas antes de su ejecución, como medida preventiva obligatoria.

Autenticación y validación de identidad

La normativa exige fortalecer los mecanismos que permiten verificar quién realiza cada operación:

- Validación de identidad del usuario en cada interacción.
- Uso de métodos de autenticación adecuados (tecnológicamente neutros).
- Confirmación obligatoria de transacciones atípicas antes de su ejecución.

Canales de atención y respuesta inmediata

Las entidades deben garantizar mecanismos efectivos de atención al usuario:

- Canales accesibles 24/7 para reportar fraudes.
- Bloqueo inmediato de productos o servicios afectados.
- Protocolos de atención a víctimas previamente definidos y validados por el regulador.

Supervisión, coordinación y sanciones

El marco regulatorio fortalece la supervisión y el control institucional:

- Coordinación entre entidades financieras, incluyendo la Superintendencia General de Entidades Financieras **(SUGEF)**, el OIJ y el **Banco Central** para la prevención e investigación de fraudes.
- Exigencia de trazabilidad y reporting de incidentes para fines regulatorios.
- Incorporación de sanciones penales en casos de autofraude o simulación de delitos.

Ley de protección de fraude electrónico en la banca

- **Mayor exposición financiera frente a fraudes electrónicos**
  Las entidades deben responder por operaciones no autorizadas, aumentando el impacto económico del fraude.
- **Necesidad de demostrar diligencia, no solo declararla**
  Los controles deben ser verificables y sostenibles ante auditorías o disputas.
- **Presión por fortalecer autenticación, monitoreo y prevención**
  Se incrementa la necesidad de adoptar tecnologías más robustas.
- **Importancia crítica de la evidencia digital y trazabilidad**
  La reconstrucción de cada operación será clave para la defensa del banco.
- **Gestión de excepciones como culpa grave del usuario o autofraude**
  Se requerirá evidencia sólida para acreditar estos casos.

Principales riesgos bajo la nueva ley

- Procesos de autenticación que no permiten validar la identidad con certeza
- Falta de evidencia verificable ante reclamos o disputas
- Baja capacidad para detectar transacciones atípicas en tiempo real

¿Cómo ayuda Sovos?

En el contexto de la nueva regulación sobre fraude electrónico en Costa Rica, las entidades financieras enfrentan un doble desafío: reducir el fraude y demostrar que actuaron con la diligencia exigida por la normativa.

Sovos apoya a los bancos en ambos frentes, fortaleciendo la validación de identidad, la autenticación de usuarios y la generación de evidencia digital para responder ante reclamos, auditorías y procesos regulatorios.

Verificación de identidad y autenticación confiable

Sovos permite fortalecer la validación de identidad en cada interacción:

- Biometría facial con prueba de vida
- Validación de identidad e integración con fuentes oficiales (según disponibilidad del banco)
- Detección de documentos alterados o identidades fraudulentas
- Aplicable en canales digitales y presenciales

Firma electrónica: evidencia y no repudio

La solución de firma de Sovos permite validar una operación y sostenerla jurídicamente ante una disputa.

- Captura evidencia completa del proceso de firma (identidad, consentimiento)
- Genera trazabilidad verificable ante auditorías o disputas
- Permite demostrar que el usuario autorizó la operación

SOVOS

Preguntas frecuentes sobre la ley de fraude electrónico en la banca en Costa Rica (Ley N° 10.889)

¿La ley obliga a usar tecnologías específicas como la biometría ?

No. La normativa es tecnológicamente neutra, pero exige controles adecuados, lo que impulsa la adopción de tecnologías más robustas -como la biometría- para prevenir, detectar y responder a fraudes.

¿El banco siempre debe responder ante un fraude?

En principio, sí. La ley establece responsabilidad objetiva. El banco solo puede eximirse si logra demostrar que actuó con la diligencia adecuada y que el fraude no fue atribuible a sus controles o procesos.

¿Qué pasa si el banco no responde dentro de los plazos establecidos?

Se generan compensaciones económicas automáticas para el usuario y, tras 120 días, pierde la posibilidad de rechazar el reclamo y debe restituir los fondos.

¿Qué tipo de controles se esperan por parte de las entidades financieras?

Controles preventivos, detectivos y correctivos: monitoreo, autenticación, validación de identidad y detección de anomalías.

¿Cómo pueden las entidades demostrar que actuaron con la diligencia adecuada?

A través de evidencia verificable de sus procesos: registros de autenticación, validación de identidad, monitoreo transaccional y trazabilidad completa de cada operación.

¿Qué rol juega la evidencia digital en este nuevo marco regulatorio?

Es clave para probar quién realizó una operación y bajo qué condiciones.

En un entorno donde la carga de la prueba recae en el banco, contar con tecnología que además de prevenir, permita demostrar, es clave.

Fortalece tus controles, reduce el fraude y cumple con la Ley 10.889.
Habla con un experto de Sovos.