SEGURIDAD DIGITAL Y PREVENCION DE ESTAFAS FINANCIERAS, RIESGOS INHERENTES EN LAS PLATAFORMAS VIRTUALES

Lic. Ernesto León Téllez

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

INTRODUCCION

Bolivia ha experimentado una acelerada transformación digital dentro de su sistema bancario y comercial. La expansión del acceso a internet mediante telefonía móvil y la bancarización de la población han impulsado el uso de canales electrónicos. Herramientas como las aplicaciones de banca móvil y la masificación de los pagos inmediatos mediante códigos QR han redefinido la forma en que los ciudadanos realizan transacciones cotidianas, dinamizando la inclusión financiera en el país.

Sin embargo, esta rápida transición tecnológica ha expuesto al ecosistema financiero a complejos desafíos de seguridad. La falta de educación digital en sectores vulnerables de la población y el surgimiento de nuevas técnicas de ciberdelincuencia han derivado en un incremento de estafas, suplantación de identidad y robos de información

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

CONCEPTOS CLAVE

Phishing, Smishing y Vishing: Modalidades de suplantación de identidad digital. El *Phishing* opera mediante correos electrónicos engañosos; el *Smishing* utiliza mensajes de texto (SMS) o mensajería instantánea como WhatsApp; y el *Vishing* se ejecuta a través de llamadas telefónicas fraudulentas. Todos estos canales buscan clonar credenciales o tokens de acceso a la banca móvil.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

CONCEPTOS CLAVE

Malware Financiero: Programas maliciosos (como troyanos o registradores de pulsaciones de teclado) diseñados para infectar dispositivos móviles o computadoras. Su meta es interceptar datos de inicio de sesión o alterar las órdenes electrónicas de transferencia de fondos.

Consumidor Financiero: Persona natural o jurídica que utiliza los servicios y productos brindados por las Entidades de Intermediación Financiera (EIF) o Empresas de Tecnologías Financieras (ETF) bajo la regulación y protección normativa de la ASFI.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

USO Y MANEJO ADECUADO DE LOS CAJEROS AUTOMÁTICOS (ATM), CARACTERÍSTICAS Y BENEFICIOS

Los cajeros automáticos (ATM) representan una infraestructura de conexión crucial entre la banca física y los sistemas de procesamiento digital en Bolivia.

Características del Servicio

Los ATM operan bajo redes de interconexión nacional (como Red Enlace o Red Libélula) que permiten la disponibilidad del servicio las 24 horas del día. Cuentan con lectores de tarjetas con tecnología de chip EMV y *contactless* (sin contacto), lectores biométricos de huella dactilar y módulos de dispensación y recepción de efectivo en tiempo real.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

USO Y MANEJO ADECUADO DE LOS CAJEROS AUTOMÁTICOS (ATM), CARACTERÍSTICAS Y BENEFICIOS

Beneficios

Proporcionan inmediatez para el retiro y depósito de dinero, consulta de saldos, cambio de clave PIN y pago de servicios básicos (agua, luz, telecomunicaciones). Eliminan la necesidad de acudir a las ventanillas de las sucursales bancarias, optimizando el tiempo del consumidor financiero y facilitando transacciones fuera del horario de atención al público.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

USO Y MANEJO ADECUADO DE LOS CAJEROS AUTOMÁTICOS (ATM), CARACTERÍSTICAS Y BENEFICIOS

Riesgos Inherentes y Recomendaciones de Uso

Entre los riesgos físicos y tecnológicos más comunes se encuentra el *Skimming* (instalación de dispositivos clonadores de bandas magnéticas y microcámaras para capturar el PIN), la colocación de "lazos libaneses" o trampas para retener tarjetas y efectivo, y el marcaje o asalto a la salida del recinto.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

BENEFICIOS, USOS, VENTAJAS Y RIESGOS DE LOS SERVICIOS DIGITALES Y ACTIVOS VIRTUALES

El ecosistema de pagos y transacciones electrónicas en Bolivia abarca diversos instrumentos regulados por el Banco Central de Bolivia (BCB) y la ASFI:

Canal / Herramienta	Usos y Ventajas	Riesgos Inherentes
Banca Electrónica y Token	Gestión integral de cuentas, transferencias e inversiones las 24/7. El Token (físico o digital) genera claves dinámicas de un solo uso que refuerzan el acceso mediante doble factor de autenticación.	Infección por troyanos bancarios, *Phishing* para la captura de credenciales y la entrega voluntaria del Token a terceros tras engaños.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

Canal / Herramienta	Usos y Ventajas	Riesgos Inherentes
Pagos y Cobros con QR	Transferencias inmediatas interoperables (QR *Simple / Método QR BCB*) sin necesidad de intercambiar datos de cuentas o usar efectivo.	*Qishing* (alteración física de códigos QR en comercios), redireccionamiento a páginas maliciosas y presentación de comprobantes de pago digitales manipulados o falsificados.
Tarjetas de Débito y POS	Pagos presenciales directos en comercios con tecnología chip o *contactless*, evitando la portación de dinero en efectivo.	Clonación de datos, robos físicos, clonación por lecturas no autorizadas en tecnología sin contacto y dobles cobros por fallas en las terminales POS.

Canal / Herramienta	Usos y Ventajas	Riesgos Inherentes
Órdenes Electrónicas de Transferencia de Fondos (OETF)	Envío eficiente de fondos entre cuentas del mismo banco o interbancarias (ACH) con trazabilidad oficial.	Errores en la digitación de la cuenta de destino o desvío de fondos por manipulación de software en el equipo del ordenante.
Billeteras Móviles	Inclusión financiera para la población sin cuenta bancaria tradicional, vinculando el número de teléfono móvil a una cuenta de dinero electrónico (ej. Yape, Tigo Money).	Suplantación de identidad mediante *SIM Swapping* (duplicado no autorizado del chip telefónico) y extravío del dispositivo sin contraseña de bloqueo.

Canal / Herramienta	Usos y Ventajas	Riesgos Inherentes
Compras por Internet	Acceso al comercio electrónico local e internacional, permitiendo el pago de servicios y productos.	Exposición de números de tarjeta y código CVV en comercios electrónicos no cifrados y robo de datos mediante tiendas virtuales falsas.
Activos Virtuales (Cripto)	Uso de criptoactivos e instrumentos tokenizados para transferencias, almacenamiento de valor y operaciones autorizadas bajo el marco del BCB y la reglamentación ETF de la ASFI.	Extrema volatilidad, ausencia de seguro de depósito, irreversibilidad de operaciones y estafas en plataformas de intercambio (*Exchanges*) no reguladas.

SEGURO DE LA BANCA ELECTRÓNICA Y BANCA MÓVIL

Para atenuar el impacto económico derivado de los delitos informáticos, las Entidades de Intermediación Financiera en Bolivia ofrecen pólizas de seguro especializadas en la protección de la banca electrónica, la banca móvil y las tarjetas.

Coberturas Principales

Estos seguros cubren pérdidas financieras causadas por transacciones no reconocidas, transferencias fraudulentas mediante la banca digital producto de *Phishing* o *Malware*, uso indebido de tarjetas por robo, hurto o clonación, y retiros forzados bajo coacción física (secuestro exprés).

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

SEGURO DE LA BANCA ELECTRÓNICA Y BANCA MÓVIL

Exclusiones y Condiciones

Las pólizas operan bajo la premisa del deber de cuidado del asegurado. No cubren eventos clasificados como negligencia grave, entre los que se incluye la entrega voluntaria de claves primarias, PIN o códigos Token a terceras personas. Para acceder a la indemnización, es obligatorio que la víctima reporte el hecho a la entidad financiera dentro de los plazos estipulados por contrato para proceder al bloqueo inmediato del canal digital o plástico.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

MEDIDAS DE SEGURIDAD PARA EL USO SEGURO DE LAS TARJETAS DE DÉBITO (ASÍ COMO CARGOS ASOCIADOS Y COMISIONES)

Las tarjetas de débito son el instrumento de pago de mayor circulación en Bolivia. Su utilización segura exige la adopción de medidas preventivas técnicas y el conocimiento del esquema operativo fijado por la ASFI.

Medidas de Seguridad

Protección del Código CVV/CVC y Datos: No compartir fotografías del reverso ni del anverso de la tarjeta. Se recomienda memorizar el código de seguridad (los tres dígitos al reverso) y mantenerlo cubierto.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

MEDIDAS DE SEGURIDAD PARA EL USO SEGURO DE LAS TARJETAS DE DÉBITO (ASÍ COMO CARGOS ASOCIADOS Y COMISIONES)

Configuración de Parámetros Operativos: Habilitar desde la aplicación de banca móvil las opciones de geobloqueo, límites diarios de gasto para compras por internet o cajeros automáticos, y encendido/apagado temporal de la función *contactless*.

Control Transaccional: Activar las notificaciones inmediatas por SMS o correo electrónico para verificar el débito exacto tras cada compra en puntos POS o portales web.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

MEDIDAS DE SEGURIDAD PARA EL USO SEGURO DE LAS TARJETAS DE DÉBITO (ASÍ COMO CARGOS ASOCIADOS Y COMISIONES)

Cargos Asociados y Comisiones

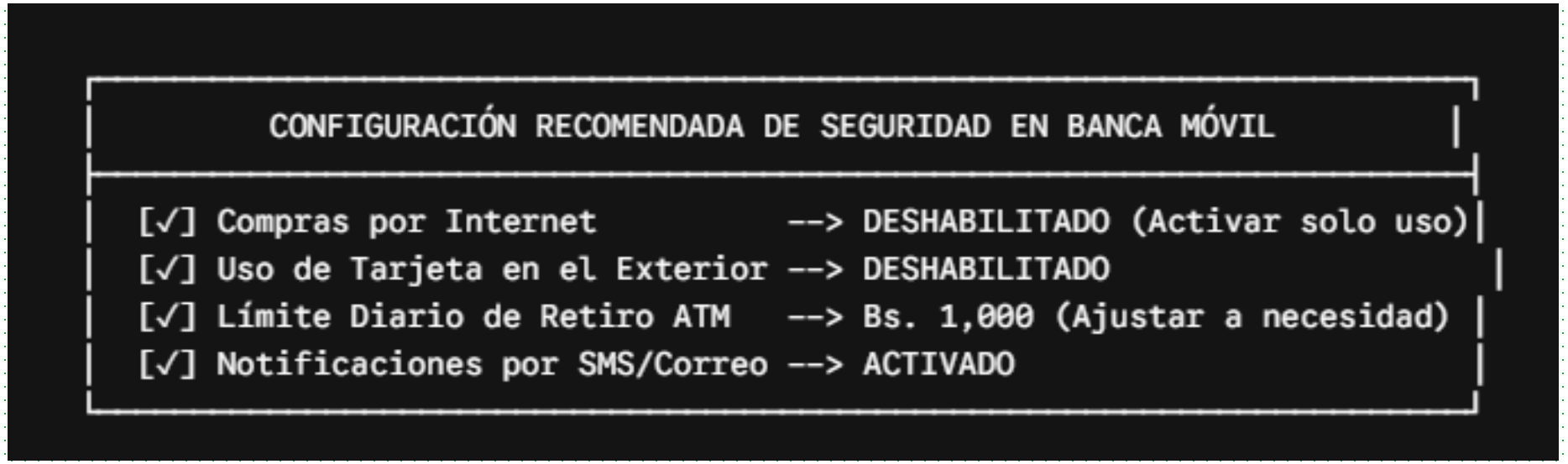
La normativa vigente dictaminada por la ASFI y el BCB regula la cobrabilidad de comisiones financieras:

Uso Nacional: Las compras presenciales en puntos POS y las transacciones en cajeros automáticos de la propia entidad no generan comisiones para el usuario. Los retiros en cajeros de otros bancos (interredes) pueden tener un número de operaciones gratuitas al mes antes de aplicar un costo estandarizado.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

MEDIDAS DE SEGURIDAD PARA EL USO SEGURO DE LAS TARJETAS DE DÉBITO (ASÍ COMO CARGOS ASOCIADOS Y COMISIONES)

Uso Internacional y Comercio Electrónico: Las transacciones para compras por internet en plataformas internacionales o consumos en el extranjero con tarjetas de débito están sujetas a los parámetros fijados por la normativa nacional, prohibiéndose el cobro de comisiones arbitrarias o recargos no autorizados por la autoridad reguladora.



Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

GUÍA PARA EL USO DE SERVICIOS ELECTRÓNICOS, RIESGOS INHERENTES Y PREVENCIÓN DE FRAUDES

El uso de canales financieros digitales requiere una postura constante de prevención y verificación por parte del consumidor financiero.

Reglas de Oro para la Prevención

Verificación Institucional: Ninguna entidad bancaria regulada por la ASFI solicita contraseñas, PIN, número de tarjeta ni códigos Token a través de llamadas telefónicas, correos electrónicos o mensajes de WhatsApp.

Conexión Segura: Acceder a la banca por internet únicamente digitando la dirección web oficial del banco en la barra del navegador, evitando el ingreso mediante enlaces patrocinados o resultados de motores de búsqueda.

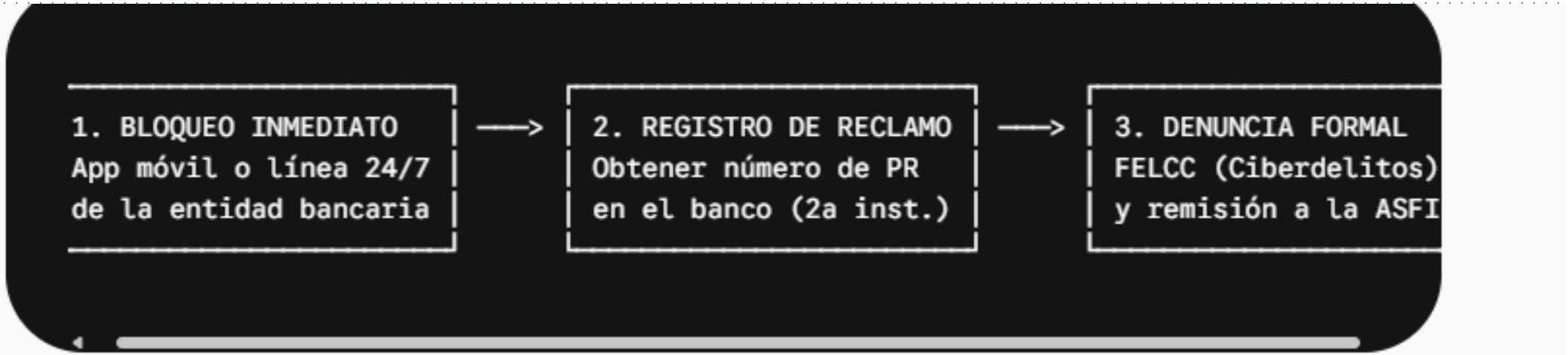
Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

GUÍA PARA EL USO DE SERVICIOS ELECTRÓNICOS, RIESGOS INHERENTES Y PREVENCIÓN DE FRAUDES

Redes y Dispositivos Privados: Realizar operaciones financieras exclusivamente desde redes privadas de datos móviles o Wi-Fi residenciales protegidas. Se debe evitar categóricamente el uso de redes Wi-Fi públicas o abiertas en lugares de alto tráfico

Protocolo de Reacción ante un Incidente de Fraude

En caso de detectar movimientos no autorizados o la vulneración de credenciales de acceso:



Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

GUÍA PARA EL USO DE SERVICIOS ELECTRÓNICOS, RIESGOS INHERENTES Y PREVENCIÓN DE FRAUDES

Bloqueo Inmediato: Ingresar a la banca móvil y bloquear de forma preventiva las tarjetas y credenciales de acceso, o llamar a la línea de atención telefónica de emergencia 24/7 de la entidad.

Presentación de Reclamo: Formalizar el reclamo de *desconocimiento de transacción* en la entidad financiera para obtener el código de Punto de Reclamo (PR).

Acción Legal e Instancia Reguladora: Si la respuesta de la entidad no es satisfactoria, acudir a la División de Delitos Informáticos de la Fuerza Especial de Lucha Contra el Crimen (FELCC) para sentar la denuncia formal y elevar el caso ante la Defensoría del Consumidor Financiero de la ASFI.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

CONTRATOS ELECTRÓNICOS, ÓRDENES ELECTRÓNICAS DE FONDOS Y MECANISMOS DEL COMERCIO ELECTRÓNICO

La validez jurídica y operativa de las transacciones digitales en Bolivia se fundamenta en un marco regulatorio específico emitido por el Estado Plurinacional, el BCB y la ASFI.

Contratos Electrónicos y Firma Digital

Los contratos de adhesión para la apertura de cuentas, la afiliación a servicios de banca por internet, billeteras móviles o la solicitud de créditos digitales se formalizan mediante mecanismos electrónicos. La normativa vigente reconoce el valor probatorio de la Firma Digital y de los métodos de autenticación explícita (como la confirmación biométrica o la aceptación de términos y condiciones en la aplicación móvil), siempre que garanticen la identidad de los firmantes y la inalterabilidad del documento contractual.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

CONTRATOS ELECTRÓNICOS, ÓRDENES ELECTRÓNICAS DE FONDOS Y MECANISMOS DEL COMERCIO ELECTRÓNICO

Órdenes Electrónicas de Transferencia de Fondos (OETF)

Las OETF constituyen las instrucciones dadas por un usuario a su entidad financiera para acreditar o retirar fondos de una cuenta de manera electrónica. El Reglamento del BCB exige que el procesamiento de estas órdenes cumpla con tres principios técnicos de seguridad obligatorios:

- **Autenticidad** (verificación positiva de la identidad del titular)
- **Integridad** (protección de los datos contra modificaciones durante el tránsito y almacenamiento)
- **Confidencialidad** (transporte de información cifrada bajo protocolos TLS/SSL).

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

CONTRATOS ELECTRÓNICOS, ÓRDENES ELECTRÓNICAS DE FONDOS Y MECANISMOS DEL COMERCIO ELECTRÓNICO

Mecanismos del Comercio Electrónico

El comercio electrónico en el país opera a través de pasarelas de pago, procesadores de tarjetas de débito/crédito e integraciones API para códigos QR inmediatos. Estas plataformas deben contar con niveles de certificación de seguridad internacionales (como PCI-DSS) e implementar la autenticación robusta mediante doble factor para validar las transacciones de compra en línea.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

RESUMEN

1. Transformación digital y adopción del pago QR

El uso de aplicaciones de banca móvil y la adopción de pagos inmediatos con código han transformado el comercio y la inclusión financiera en el país.

2. Prevalencia de la Ingeniería Social sobre los ataques técnicos

A través de la **ingeniería social**, los delincuentes manipulan a las víctimas utilizando modalidades como el *Phishing* (correos falsos), *Smishing* (mensajes de WhatsApp/SMS) y *Vishing* (llamadas telefónicas) para obtener voluntariamente contraseñas y tokens.

3. Riesgos híbridos en los Cajeros Automáticos (ATM)

Persisten riesgos físicos y tecnológicos como el *Skimming* (dispositivos para clonar bandas magnéticas y capturar el PIN), por lo que se exige la revisión visual del equipo y el bloqueo de la vista al digitar la clave.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

RESUMEN

4. Seguridad de la Banca Móvil y el rol fundamental del Token

La operaciones están respaldadas por la **Autenticación de Doble Factor (2FA)** mediante Tokens físicos o digitales que generan claves dinámicas de un solo uso. La vulneración de este canal casi siempre ocurre cuando el usuario revela este código temporal bajo engaños de supuestos premios o bloqueos de cuenta.

5. Estafas en transacciones con Código QR (*Qishing*)

El uso masivo del QR ha generado nuevas modalidades de estafa: el *Qishing* (alteración de códigos QR impresos en comercios para desviar fondos) y el uso de comprobantes de pago digitales manipulados o falsificados

6. Billeteras móviles e integración de Activos Virtuales (Cripto)

Plataformas como las billeteras móviles facilitan la inclusión de personas sin cuenta bancaria tradicional, aunque enfrentan riesgos de *SIM Swapping* (clonación del chip telefónico).

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

RESUMEN

7. Cobertura restringida de los Seguros Bancarios

Los seguros contra fraude en banca electrónica y tarjetas cubren pérdidas por robos, clonación (*skimming*), transferencias por virus (*malware*) y asaltos. Sin embargo, las pólizas **excluyen los fraudes por negligencia grave o la entrega voluntaria de claves**, dejando desprotegido al usuario que entrega su Token o clave primaria a un estafador.

8. Protocolo de reacción inmediata ante fraudes

Ante cualquier transacción sospechosa o robo de dispositivo, el usuario debe actuar bajo un protocolo en tres pasos: **1)** Bloqueo inmediato de accesos y plásticos a través de la App o línea 24/7 del banco; **2)** Presentación de reclamo formal (*desconocimiento de cargos*) solicitando su código de Punto de Reclamo (PR); y **3)** Denuncia ante la División de Ciberdelitos de la FELCC y posterior escalamiento a la ASFI si la entidad no da respuesta.

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.

GRACIAS POR SU ATENCION

Cacsa
Cooperativa de Ahorro y Crédito Abierta San Antonio R.L.