COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Medidas de seguridad en transacciones financieras

Comisión de Hacienda del Senado

Solange Berstein
Presidenta
Comisión para el Mercado Financiero

Lunes 18 de marzo 2024

Marco Regulatorio para Emisores

Marco General de Gestión de Riesgo

- Modelo de **supervisión basado en riesgo** de CMF exige a los emisores fiscalizados (bancos, emisores de tarjetas no bancarios y cooperativas, entre otros, incluyendo recientemente Fintec) contar un sistema de gestión de riesgo integral y, particularmente, de gestión de riesgo operacional, el cual dependerá de la naturaleza, complejidad y volumen de las operaciones.

- **Normas específicas de CMF asociadas al riesgo operacional** de las entidades, incluyen: externalización de servicios, incidentes operacionales, continuidad operacional, y seguridad de la información y ciberseguridad.

- En el ámbito de la **autenticación y medidas de seguridad**, la Norma entrega un marco de aplicación general para todos los medios de pagos, algunas exigencias más específicas, para los pagos realizados por medio de transferencias electrónicas de fondos (TEF).

Ver: Gestión de Riesgo: Recopilación Actualizada de Normas, RAN 1-13; Circular N°1 de Emisores de Tarjetas; Circular N°108 de Cooperativas). Riesgo operacional: RAN 20-7, RAN 20-8, RAN 20-9, RAN 20-10. Servicios Fintec, NCG N°502. Autenticación RAN 1-7.

Resumen exigencias generales sobre seguridad y autenticación

Se aplica a los servicios electrónicos de comunicación de pagos con transferencias, tarjetas y cajeros automáticos. Así también, la RAN 1-7 se hace extensiva a bancos, cooperativas, emisores de tarjetas no bancarias, operadores y sociedades de apoyo al giro.

- **Contrato de prestación de servicios** entre la entidad y el cliente (derechos y responsabilidades).
- **Registro y trazabilidad de las operaciones** y generación de archivos que permitan su examen posterior (fecha, hora, emisor, operador, monto, entre otros).
- **Perfil de seguridad** que garantice que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resguardar, además, la privacidad o confidencialidad de la información transmitida o procesada por ese medio.
- **Procedimientos que permitan asegurar la autenticidad e integridad de las operaciones**, debiendo utilizarse métodos de autentificación para el acceso al sistema.
- **Canales de comunicación que permitan bloqueo** de operaciones y aviso en caso de hurto, robo, extravío o fraude por parte del usuario en cualquier momento.
- **Mecanismo de continuidad de operaciones**, respaldo y detección de operaciones fraudulentas
- **Limites a las operaciones** y controles de saldos.
- **Generación de comprobantes** de la transacción al cliente y disponibilidad de cartola de transacciones.

Normativa sobre métodos de autentificación

Las normativas de la CMF y del Banco Central de Chile exigen contar con métodos de autentificación para el acceso al sistema, que permitan asegurar su autenticidad e integridad.

- **Transferencias electrónicas interbancarias**
  - Los bancos deben disponer que las **transferencias se cumplan en forma inmediata.**
  - Se debe contar con una plataforma tecnológica que comprenda una **encriptación** sólida, disponer de a lo menos **dos factores de autentificación** distintos para cada transacción, debiendo ser **uno de ellos de generación o asignación dinámica**; establecer la exigencia de firma digital avanzada para las transferencias superiores a un monto que el banco determine.

- **Tarjetas de pago**
  - Las exigencias regulatorias comprenden, entre otras disposiciones, como mínimo contar con "*una tecnología de seguridad que permita proteger apropiadamente la información contenida en las Tarjetas, implementar mecanismos robustos de autentificación y prevención de fraudes, así como facilitar la verificación oportuna de la disponibilidad de cupos y saldos de éstas, y su bloqueo. Adicionalmente, medidas para continuidad de servicio y alta disponibilidad*".

Medidas para detectar y prevenir fraudes

- Contar con sistemas para identificar, evaluar, monitorear patrones de fraude; para marcar o abortar actividades u operaciones potencialmente fraudulentas.

- Estos sistemas o mecanismos deberán permitir tener una vista integral y oportuna de las operaciones del cliente, del no cliente (por ejemplo en los intentos de acceso), de los puntos de acceso (por ejemplo direcciones IP, Cajero Automático u otros), hacer el seguimiento y correlacionar eventos y/o fraudes a objeto de detectar otros fraudes, puntos en que estos se cometen, modus operandi, y puntos de compromisos, entre otros.

- Deben controlar que los importes girados no superen el saldo disponible o el límite que se haya fijado para el efecto. En el caso de las TEF, debe establecerse un límite en los montos de transferencia con respecto a cada cliente con acceso al sistema.

=> Todas estas medidas de autenticación y para prevenir fraudes, buscan asegurar la firmeza de las operaciones, protegiendo la cadena de pagos y al mismo tiempo, protegiendo a las personas de eventuales fraudes.

Proceso de Supervisión

En el ámbito prudencial, la CMF supervisa los **riesgos operacionales y tecnológicos,** a través de un enfoque basado en riesgos

Evaluación de Gestión: Pilares y Principios

- Rol del Directorio
- Estructura de Comités

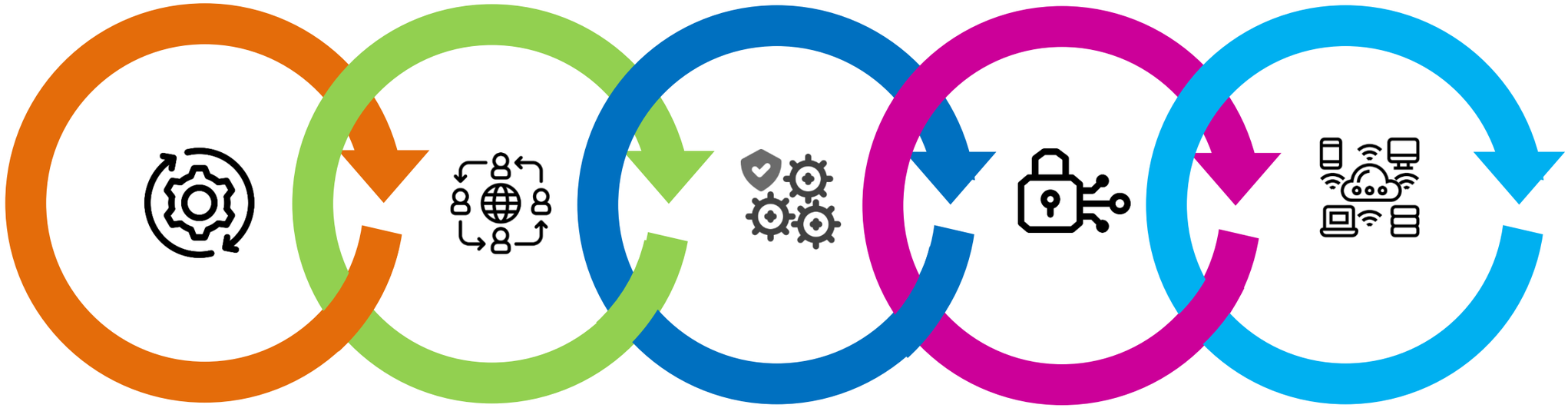
- Políticas
- Procedimientos

- Rol del Auditoría

- Función de Riesgos competente.
- Herramientas de identificación
- Metodologías de cuantificación y medición

Proceso de Supervisión

La **Gestión del Riesgo Operacional y Tecnológico** considera los siguientes ámbitos:



Riesgo de Procesos

Servicios Externalizados

Continuidad del Negocio

Seguridad de la Información

Riesgos Tecnológicos

Principales Métodos de Autenticación

En el sistema bancario chileno los métodos utilizados para autenticar la identidad de los usuarios son los siguientes:

Contraseñas y PIN

Contraseña:
Secuencia de caracteres alfanuméricos..

PIN:
Caracteres numéricos.

Biometría

Utiliza características físicas o comportamientos únicos del usuario, como huellas dactilares, reconocimiento facial, iris o voz.

Token de Seguridad

Dispositivos físicos o aplicaciones móviles que generan códigos únicos que deben ser ingresados junto con las credenciales de inicio de sesión para autenticar la identidad del usuario.

Múltiples Factores (2FA – MFA)

Combina dos o más métodos de autenticación, como una contraseña y un código de verificación enviado al teléfono móvil del usuario, para aumentar la seguridad.

Supervisión aplicada a la apertura de cuentas digitales (Onboarding)

Oferta

Creciente oferta de cuentas con apertura 100% digital.

Inclusión

Inclusión financiera.

Riesgos

Eventual riesgo de suplantación de identidad y/o fraude.

Clientes

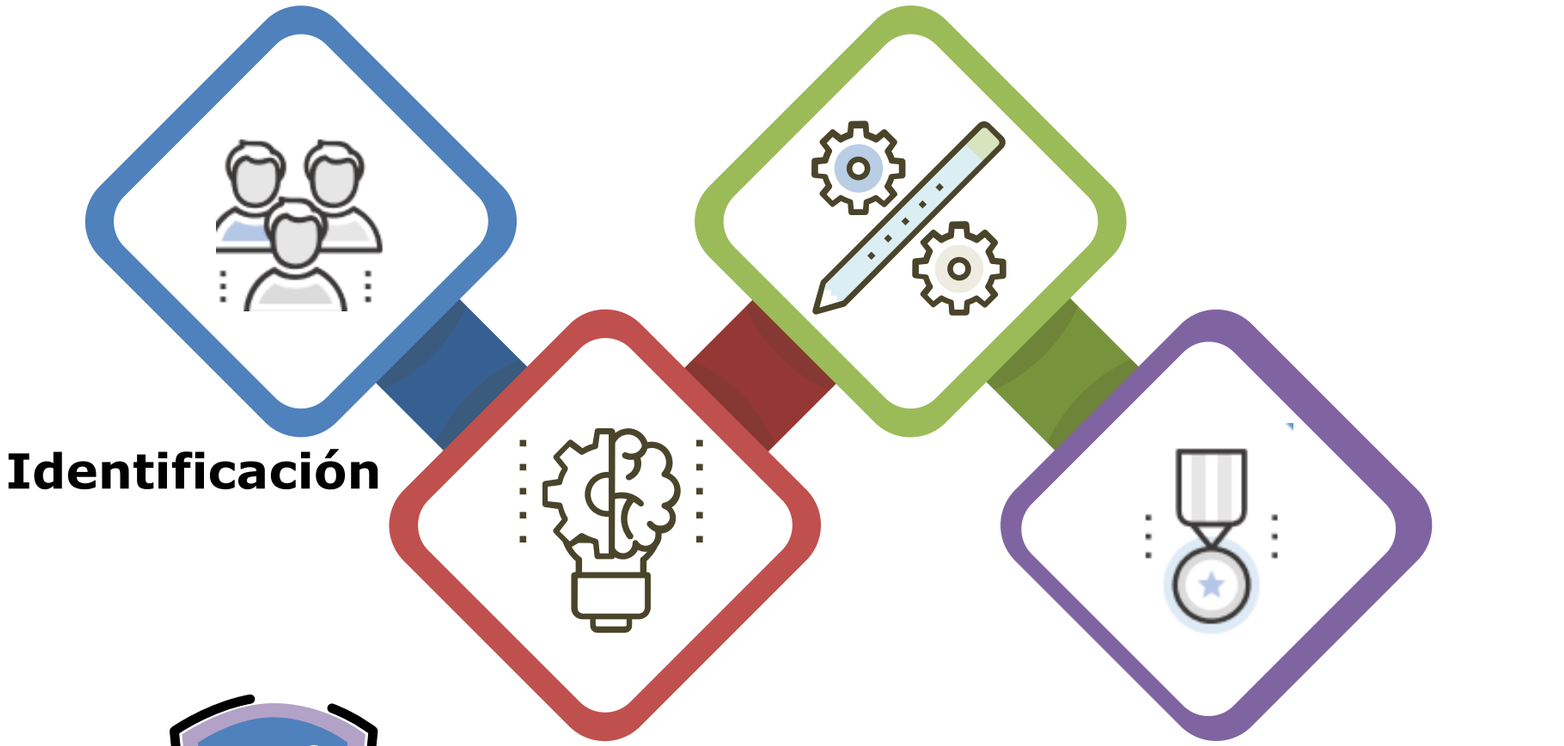
Posible afectación monetaria, reputacional, legal.

"El onboarding de un cliente es un proceso electrónico que permite su identificación frente a una institución financiera y con una confianza equivalente a la de un proceso presencial. Asimismo, lo destaca como un aspecto clave para avanzar en la digitalización y en la inclusión financiera, por cuanto se convierte en la puerta de entrada de los consumidores al sistema financiero".

(*) BID. 2021. Onboarding digital.

Proceso de apertura de cuentas digitales

Documentos y firma digital



Identificación

Autenticación

Confirmación y activación

Un proceso robusto requiere del uso de más de una validación.

Entre los procesos que se realizan durante el ***onboarding* digital**, se encuentran los mecanismos de **autenticación (verificación) de identidad** para la apertura. Estos corresponden a distintos métodos de seguridad que implementan las entidades con el fin de verificar la correcta identidad del cliente que se encuentra abriendo la cuenta.

Proceso de apertura de cuentas digitales (cont.)

Estándares de verificación de identidad

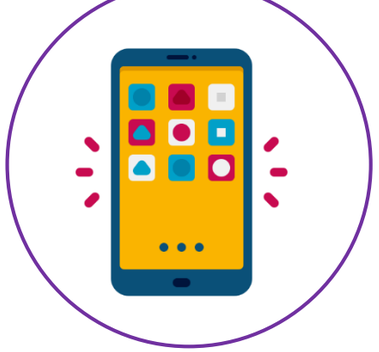
✓ Existencia de una variedad de métodos utilizados en el *onboarding*, con distintos niveles de robustez, por lo que las entidades complementan unos con otros.

Métodos de verificación de identidad para Cuentas Corrientes digitales
Número de serie de carnet de identidad
Scanner/Foto carnet de identidad
Biometría o validación facial
Clave única
Clave acceso
Preguntas de información personal
Firma electrónica simple
Autorización a través de APP específica / Clave dinámica
Otros métodos (por ej., Firma electrónica avanzada)

Supervisión proceso de transacción: Canales

Enfocando particularmente el ámbito de seguridad y autenticación, es relevante dar una visión de los canales de atención electrónicos más utilizados por los clientes para realizar transacciones de dinero:

Sitios Web



Aplicaciones Móviles

ATM

POS

Medidas de Seguridad

En el proceso de autenticación de clientes los bancos han implementado diversas medidas de seguridad, que para un mejor entendimiento podemos diferenciarlas en:

- **Medidas de Prevención**

- **Medidas de Protección**

- **Medidas de Detección y Monitoreo**

- **Medidas de Respuesta**

Medidas de Prevención

Educación y concientización de los clientes sobre prácticas seguras de autenticación

- Sección de seguridad y campañas en sitio público.

- Campañas educativas a clientes: las que pueden ser vía correo electrónico, redes sociales, mensajería SMS y aplicaciones (*push*), entre otros.

Medidas de Protección

De autenticación

- Para las TEF, se utilizan:
  - **Claves fijas** (Password y PIN)
  - **Claves dinámicas** generadas a través de un *hard-token* (*Digipass* o tarjeta de coordenadas), *soft-token* (*apps*) y/u OTP (*one time password*)
  - **Biometría** en Apps

- **Para transacciones realizadas con tarjetas de pago**, se utiliza una clave fija, uso de estándar 3D security y tecnología chip (EMV).

- **Para transacciones en ATM** (Tarjetas, Password y PIN)

Mitigadoras

- Bloqueo preventivo de cuentas y claves de acceso ante la detección de comportamientos fraudulentos
- Listado de destinatarios para transferencias habituales
- Límites de monto por transacción o límites diarios para realizar TEF o retiro de efectivo de ATM.
- Uso de Antiskimmer en ATMs para mitigar clonación de tarjetas.
- Configuración personalizada para limitar montos y áreas geográficas donde se pueden utilizar las tarjetas.
- Habilitación o deshabilitación en línea, vía *web* o móvil, de las tarjetas (*on-off*).
- Uso de chip en tarjeteas.

Medidas de Detección y Monitoreo

- Realización periódica de ejercicios de *Ethical hacking y Pentesting*.
- Herramientas para la identificación de sitios *Web* falsos.
- IPS: Uso de herramientas *Anti Hacking* que monitorea el tráfico de red y/o actividades de un sistema, en busca de actividad maliciosa
- *Firewall: de perímetro de la red, de bases de datos y de aplicativos*
- QA de calidad y seguridad en desarrollo Apps
- DLP (*Data Loss Prevention*): Permiten proteger los datos de forma proactiva y garantizar la creación de directivas eficaces de protección de la información
- Protección DDoS: protege de ataques de denegación de servicio
- *Uso antivirus, anti-malware y antispam de correo malicioso*

Medidas de respuestas

- ❑ Indisponibilizar sitios *web* falsos que simulan páginas reales de los bancos.
- ❑ Bloqueo de productos a través de *call center,* páginas *web* y aplicativos móviles
- ❑ Gestión de incidentes de seguridad

Consideraciones Finales

- El proceso de autenticación es dinámico en virtud del desarrollo de nuevas tecnologías y la contención de nuevos riesgos. En este contexto, es fundamental para proteger la información sensible de los usuarios y prevenir fraudes.

- Junto con lo anterior, un elemento relevante es el deber de cuidado y diligencia que los usuarios adopten.

- Lo anterior, sin perjuicio del cumplimiento de los mejores estándares de seguridad por parte de las instituciones financieras.

- En el futuro, se espera que la autenticación segura evolucione hacia métodos más sofisticados y sin fricción, como la autenticación continua basada en comportamiento del usuario y la autenticación sin contraseña.

- En todo caso, estas medidas no impiden que se configuren situaciones de auto-fraude, ya que no están diseñadas para ello.

COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Medidas de seguridad en transacciones financieras

Comisión de Hacienda del Senado

Solange Berstein
Presidenta
Comisión para el Mercado Financiero

Lunes 18 de marzo 2024

TIPOS DE FRAUDE MÁS COMUNES

Clonación

Método por el cual a través de un aparato Skimmer se obtiene la información de la banda magnética de una tarjeta con el fin de crear una copia de la misma, la cual insertada en una nueva tarjeta permite comprar en comercios de forma presencial.

Robo

Fraude en el cual un cliente sufre el hurto de sus tarjetas o dispositivo móvil, donde el delincuente genera compras con la tarjeta física del cliente y en el caso de su dispositivo móvil, este es robado desbloqueado y muchas veces las personas mantienen sus claves escritas en sus notas, y utilizando estas claves se generan operaciones financieras desde el propio dispositivo del cliente defraudado, usualmente se concreta el fraude mediante transferencias electrónicas de fondos y compras por internet.

Fraude amigable

Fraude en el que el cliente desconoce una transacción originada con su consentimiento, pero muchas veces no conoce la procedencia del cargo producto de glosas poco claras, productos no entregados por el comercio o muchas veces por que olvidó que realizo ciertas compras.

Phishing

Método de fraude en el que un estafador envía una serie de SMS/Correos a una base de datos de números o emails los cuales contienen links maliciosos en los que usurpando la imagen de alguna entidad financiera solicitan datos personales a los clientes, tales como números de tarjeta, fecha de vencimiento, CVV2, y la mayoría veces también RUT y clave internet de su entidad, últimamente también han solicitado un segundo factor de autenticación con el fin de enrolar la aplicación del banco en un nuevo dispositivo o enrolar tarjetas en Wallets tales como Apple Pay y Google Pay.

Auto fraude ATM

Situación en la que el mismo cliente, haciendo un previo abono a su cuenta, solicita a un tercero conocido por el hacer un Giro en cajero Automático con el fin de desconocer la operación en su entidad financiera para que el banco haga la restitución de los fondos y de cierta manera, duplicar el dinero.

Ingeniería social

Técnicas por las cuales un estafador logra convencer a los clientes de entregar sus datos personales tales como RUT, claves de internet y segundo factor de autenticación de la entidad financiera con el fin de apoderarse de los canales digitales de los clientes para posteriormente generar operaciones financieras sin conocimiento del dueño de la cuenta. Un ejemplo usual de esto es el conocido cuento del tío y también la restitución de fondos por concepto de intereses.

Transacciones por internet

Fraudes por los cuales utilizando robots se prueban rangos de tarjeta y combinaciones de fecha de vencimiento y CVV2 con el fin de encontrar tarjetas validas con sus datos para posteriormente materializar el fraude mediante compras en sitios web.

Proceso de apertura de cuentas digitales (cont.)

Estándares de verificación

- ✓ Existencia de una variedad de métodos utilizados en el *onboarding*, con distintos niveles de robustez, por lo que las entidades complementan unos con otros.
- ✓ De los mecanismos utilizados por las entidades en la **verificación de identidad, e**n un 62% de las cuentas digitales se utiliza la Biometría o Validación Facial.