FRAUDES VIRTUALES EN EL SISTEMA FINANCIERO

Dr. Jorge Arturo Gómez

- Instituto de Capacitación Judicial de las Provincias Argentinas y CABA – REFLEJAR / JUFEJUS
- Consejo de Procuradores, Fiscales, Defensores y Asesores Generales de la República Argentina
- Consejo Federal de Política Criminal de la República Argentina


Fraudes Bancarios
E-bank
Vishing
Token
IMEI
CBU
IP
Banca Movil (mobile)
CVU
Fintech
Pishing
On Line Baking
BCRA
Tarjeta de Coordenadas
Ciberseguridad
Banca Electrónica
Riegos
Home Banking (HB)
Pandemia Covid-19
Debin
Canales Electrónicos
Ecosistema Informático
Préstamos On Line
Cajeros Automáticos (ATM)
Credulidad - Exceso de Confianza
Divulgación Credenciales y Claves
Inclusión Financiera
Vulnerabilidad
Capacitación - Concientización
Medios de Pagos Electrónicos

Normas del Banco Central de la República Argentina (BCRA) sobre Ciberseguridad para el Ecosistema Financiero

Comunicación A-6017 BCRA – 15/07/2016 y modif.: Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras.

Comunicación A-7072 BCRA – 16/07/2020: Sistema Nacional de Pagos –Transferencias - Recaudos especiales sobre transferencias en moneda extranjera. _

Comunicación A-7319 BCRA – 01/07/2021: Adecuación de los "Requisitos mínimos de gestión, implementación y control de riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras.

Comunicación A- 7266 BCRA - 16/04/2021: Lineamientos para la respuesta y recuperación ante ciberincidentes (RRCI).

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

“Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”

Servicios financieros por los siguientes Canales Electrónicos (CE):

- Cajeros Automáticos (ATM)
- Terminales de Autoservicio (TAS)
- Banca Móvil (BM)
- Banca Telefónica (BT)
- Banca por Internet (BI)
- Puntos de Venta (POS)
- Plataforma de Pagos Móviles (PPM).”

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

Glosario de términos utilizados:

Autenticación Fuerte - Doble Factor: Utilización combinada de dos factores de autenticación, es decir dos elementos de las credenciales de distinto factor.

Banca Electrónica: Todo servicio bancario y/o financiero ofrecido por una entidad, basado en el uso de tecnología para la ejecución de operaciones y transacciones por parte de un usuario de servicios financieros.

Banca Móvil (BM): Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio basado en la utilización de aplicaciones (programas) informáticas diseñadas para su implementación y operación en dispositivos móviles del usuario, que vinculan al dispositivo, la aplicación y las credenciales del cliente de manera única con una plataforma de servicios financieros, en un centro de procesamiento de la entidad (propio o de un tercero), mediante redes públicas de comunicación aptas y aprobadas por autoridad competente para la transmisión de voz y datos.

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

Banca por Internet (BI): Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros, que se basan en la utilización de programas informáticos diseñados para su **operación mediante el acceso a sitios publicados en Internet**, bajo administración de una entidad u operador y el uso de motores de navegación instalados en dispositivos el usuario.

Banca Telefónica (BT): Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros, que se basan en la utilización de programas informáticos diseñados para su **operación con teléfonos propiedad o no del consumidor financiero** y que se comunican con un centro de procesamiento de la entidad (propio o de un tercero) mediante redes públicas de comunicación aptas y aprobadas por autoridad competente para la transmisión de voz y datos bajo administración de un operador público o privado.

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

Cajeros Automáticos (ATM): Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros, que se basan en la utilización de los dispositivos conocidos cómo Cajeros Automáticos o ATM (“Automated Teller Machine”) en sus distintas modalidades: Dispensadores de Efectivo, Kioscos Digitales, entre otros y que permitan por lo menos, la extracción de efectivo sin intervención de un operador humano.

Canales Electrónicos (CE): Comprende a los medios, dispositivos, redes y servicios informáticos dispuestos por las entidades financieras, por sí o por intermedio de terceros en calidad de prestadores asociados, **para la instrucción de operaciones bancarias, con efecto sobre las cuentas de uno o más usuarios de servicios financieros y/o clientes** de esas entidades.

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

Contraseña: Elemento de las credenciales basado en una pieza de información compuesta por una **secuencia de caracteres o símbolos** sólo conocidos por el usuario tenedor *(factor basado en "algo que sabe")* o generados por un dispositivo *(factor basado en "algo que tiene")*.

Control Dual: El proceso utiliza dos o más participantes de forma separada (individuos, organizaciones, entre otros), quienes operan en forma concertada para proteger funciones o información de carácter confidencial, asegurando que **ningún participante podrá llevar adelante la función sin la intervención del resto de los participantes**.

Credenciales: Comprende a todos los elementos físicos o lógicos provistos por la entidad/operador, necesarios para algunas o todas las siguientes acciones durante el uso de un Canal Electrónico específico: *presentación/identificación, autenticación, solicitud, verificación, confirmación/autorización*.

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

Datos personales públicos: Comprende datos de personas físicas que pueden obtenerse de fuentes públicas, tales como nombres y apellidos, fechas de nacimiento, números de identificación nacional y laboral, entre otros.

Dispositivos: Comprende a los elementos físicos específicamente diseñados y dispuestos para la interacción directa entre los clientes y el Canal Electrónico. Incluye los elementos lógicos y/o aplicaciones necesarios para brindar funcionalidad y operación a los elementos físicos.

Factores de Autenticación: Las credenciales utilizadas en los CE pueden ser del siguiente tipo o factor: **“algo que sabe”**, (Contraseña, dato personal, entre otros), **“algo que tiene”** (Tarjeta TC/TD, Token, entre otros), **“algo que es”** (Característica biométrica).

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

Identificación positiva: Comprende a los **procesos de verificación y validación de la identidad** que reducen la incertidumbre mediante el uso de técnicas complementarias a las habitualmente usadas en la presentación de credenciales o para la entrega o renovación de las mismas. Se incluyen pero no se limitan a las acciones relacionadas con: **verificación de la identidad de manera personal, mediante firma holográfica y presentación de documento de identidad, mediante serie de preguntas desafío de contexto variable**, entre otros.

Journal o Tira de auditoría: Registro de la actividad de los dispositivos de los Canales Electrónicos asociados al acceso a los servicios e instrucción de operaciones.

Kiosco digital: Comprende a los dispositivos con emplazamiento y características físicas similares a los ATM (“Automated Teller Machine”) que prestan una gama de servicios mayor a la dispuesta para estos, incluyendo pero no limitándose a los servicios ofrecidos por los TAS.

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

Medios de Pago en Canales Electrónicos: Comprende a los medios o elementos físicos o electrónicos representativos y útiles para la concertación de operaciones financieras en Canales Electrónicos, que incluyen, pero no se limitan a: tarjetas de pago, débito o crédito.

Operaciones "en línea" o "fuera de línea": La operatoria "en línea" ocurre cuando la actividad del servicio o canal electrónico se encuentra en **estado activo sincrónico** entre los distintos puntos de autorización y respuesta, el dispositivo y el operador y/o entidad financiera, siendo **que en cada transacción se perfeccionan la validación, autenticación y confirmación de credenciales y transacciones financieras**.

La operatoria "fuera de línea" ocurre cuando la actividad del servicio o canal electrónico se encuentra en estado asincrónico entre los distintos puntos de resolución de autorización y respuesta, siendo necesario el perfeccionamiento de la validación, autenticación y confirmación de credenciales independientemente del momento de la validación, autenticación y confirmación de la transacción financiera.

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

Plataforma de Pagos Móviles (PPM): Aplicación o servicio informático para todo tipo de **dispositivos móviles y computadores personales** propios del usuario, que permite la asociación de tarjetas bancarias vinculadas a su vez a cuentas de crédito o débito, sin límite de número, entidades u operadores, para **la instrucción de pagos y transferencias** mediante crédito **a cuentas de terceros** adheridos o **transferencias inmediatas en cuentas a la vista.**

Servicios Financieros: Incluye la prestación de operaciones bancarias, cambiarias y/o financieras, de instrucción legal por medio bancario o pago de bienes y servicios.

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

Sesión en Canales Electrónicos: Comprende al período durante el cual un consumidor financiero (persona o comercio) puede llevar a cabo transacciones financieras, operativas o consultas permitidas en un Canal Electrónico. Esta compuesto por las siguientes etapas:

- **Presentación** (Ingreso de Credenciales, también referido como Inicio de Sesión);
- **Autenticación** (Validación y autenticación de los valores de las credenciales ingresados);
- **Solicitud** (Selección de la opción o transacción elegida),;
- **Verificación** (Etapa alternativa para la verificación de la identidad y reválida de credenciales ante determinado tipo o características de la transacción elegida);
- **Confirmación** (Validación y autorización de la transacción y cierre de ciclo).

Las etapas mencionadas son consecutivas con excepción de la **etapa de Autenticación**, que puede ocurrir continuando la etapa de solicitud y antes de la etapa de Verificación.

Comunicación A-6017 BCRA – 15/07/2016 y modif.:

Las entidades deben **desarrollar, planificar y ejecutar un plan de protección** de sus activos, procesos, recursos técnicos y humanos relacionados con los Canales Electrónicos, que debe comprender:

- Concientización y Capacitación: Programa de concientización y capacitación de seguridad informática,

- Control de Acceso: Mecanismos para la verificación de la identidad de los usuarios internos y externos, estableciendo una estrategia basada en la interoperabilidad del sistema financiero, la **reducción de la complejidad de uso y la maximización de la protección del usuario** de servicios financieros.

- Integridad y Registro: Las entidades deben **garantizar un registro y trazabilidad** completa de las actividades de los Canales Electrónicos en un entorno seguro para su generación, almacenamiento, transporte, custodia y recuperación.

Comunicación A-7072 BCRA – 16/07/2020: Sistema Nacional de Pagos –Transferencias - Recaudos especiales sobre transferencias en moneda extranjera _

Recaudos especiales previos para efectivizar una transferencia a cuentas que presenten estas características:

- Cuentas de destino que no hayan sido previamente asociadas por el originante de la transferencia a través de cajeros automáticos o por cualquier otro mecanismo;
- Cuentas de destino que no registren una antigüedad mayor a 180 días desde su apertura.
- Cuentas que no hayan registrado depósitos o extracciones en los 180 días anteriores a la fecha en que sea ordenada la transferencia inmediata.
- Cuentas de destino nominadas en moneda extranjera a partir de una segunda transferencia recibida durante el mes calendario.

En caso de no producirse la justificación del movimiento la entidad receptora deberá proceder al **rechazo de la transferencia**. La entidad podrá exceptuar las cuentas que por su propia actividad puedan justificar la recurrencia de esta operatoria.

Comunicación A-7319 BCRA – 01/07/2021: Adecuación de los “Requisitos mínimos de gestión, implementación y control de riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”

Requisitos para autorizar créditos pre aprobados:

- Verificar fehacientemente la identidad de la persona usuaria de servicios financieros involucrada, mediante **técnicas de identificación positiva**, de acuerdo con la definición prevista en el glosario.
- Constatar previamente a través del proceso de monitoreo y control, como mínimo, que los puntos de contacto indicados por el usuario de servicios financieros no hayan sido modificados recientemente.
- Verificar la identidad del usuario y comunicarle –a través de todos los puntos de contacto disponibles– que el crédito se encuentra aprobado y que, de no mediar objeciones, será acreditado en su cuenta a partir de las 48 horas hábiles siguientes. Este plazo podrá reducirse en caso de recibirse la conformidad del usuario de servicios financieros de manera fehaciente.
- Aplicable a todas las operaciones de créditos preaprobados realizadas por los canales electrónicos disponibles –ATMs, TAS, banca de internet (BI) y banca móvil (BM)–.

Lineamientos del BCRA sobre ciberseguridad:

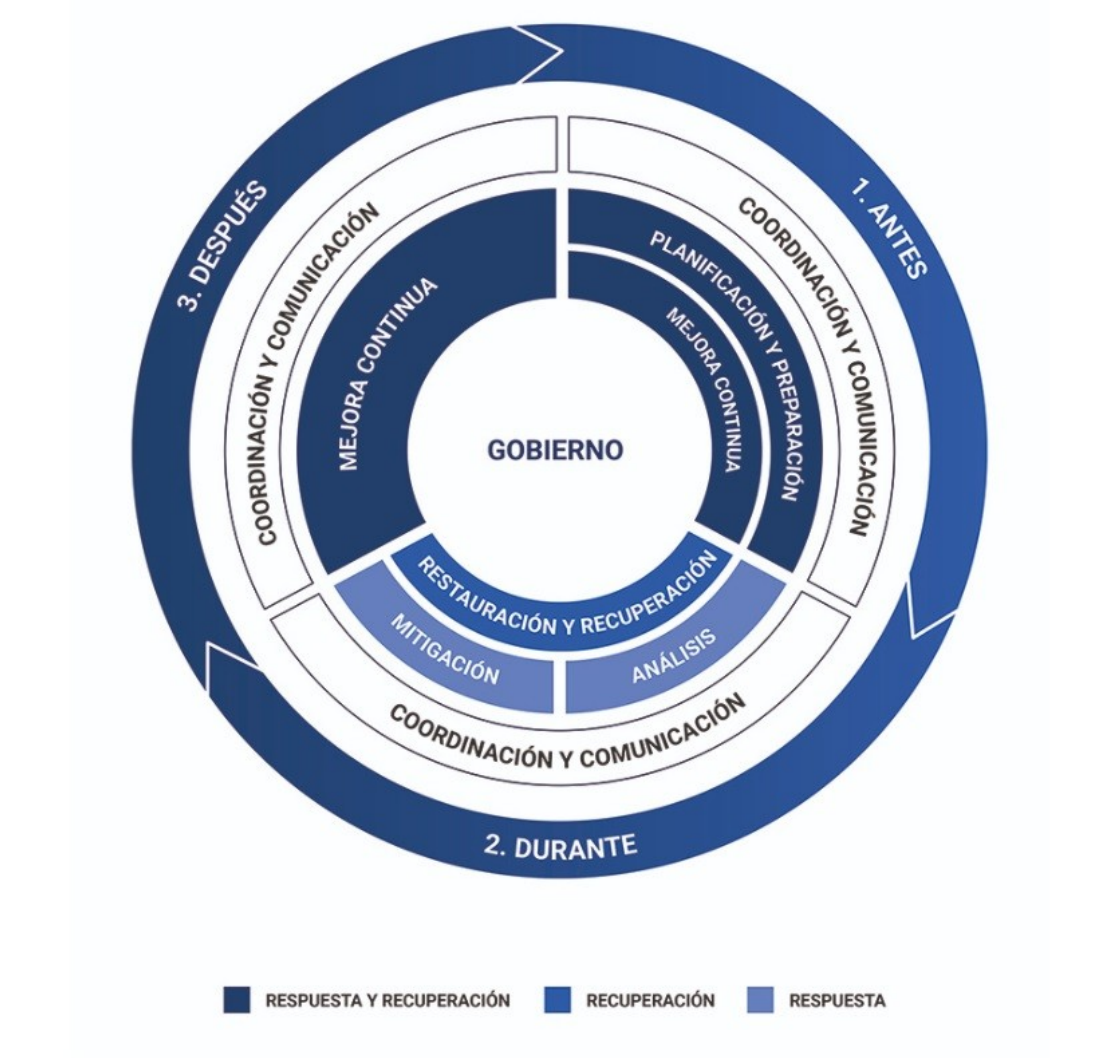
Tienen por objeto promover una planificación que aborde los nuevos desafíos y riesgos asociados a la expansión digital de los servicios financieros por medios digitales, con nuevas tecnologías y una creciente interconexión entre quienes participan del sistema financiero, sean no regulados por el Banco Central, como entidades financieras, entes operadores de redes, cámaras compensadoras, terceros prestadores de servicios, Fintechs, entre otros.

Los lineamientos dictados por el Banco Central son definimos como una guía para que se aborden los **desafíos actuales de la ciberseguridad en la planificación estratégica en el gobierno y la gestión** de las instituciones, de manera que se analice, madure y/o adopten paulatinamente estas actividades.

Esos lineamientos tienen como objetivo incorporar en la planificación estratégica de cada organización la **ciberseguridad** y la **ciberresiliencia**.

- **Lineamientos para la respuesta y recuperación ante ciberincidentes (RRCI)** (Comunicación A- 7266 - 16/04/2021), para limitar los riesgos en la estabilidad financiera e impulsar la ciberresiliencia del ecosistema en su conjunto:
    - Gobierno
    - Planificación y preparación
    - Análisis
    - Mitigación
    - Restauración y recuperación
    - Coordinación y comunicación
    - Mejora continua

Comunicación A- 7266 BCRA - 16/04/2021:



CIBERRESILIENCIA: Capacidad de una organización de anticiparse y adaptarse a ciberamenazas y otros cambios relevantes en el entorno, resistiendo, conteniendo y recuperándose rápidamente de ciberincidentes.

CIBERSEGURIDAD: Preservación de la confidencialidad, la integridad y la disponibilidad de la información y/o de los sistemas de información a través del medio cibernético (autenticidad, trazabilidad, no repudio y confiabilidad). Normas ISO/IEC 27032:2012

INGENIERÍA SOCIAL (social engineering): Acción de intentar engañar a las personas con el fin de que revelen información o realicen determinadas acciones.

TRAZABILIDAD (accountability): Propiedad que asegura que las acciones de una entidad puedan ser rastreadas y atribuidas de manera inequívoca a dicha entidad (Fuente: ISO/IEC 2382:2015)

CIBERNÉTICO (cyber): Relativo a una infraestructura tecnológica interconectada en la que interactúan personas, procesos, datos y sistemas de información (Fuente: Glosario de Ciberseguridad del BCRA)

CIBERINCIDENTE: Evento cibernético que: **i)** pone en peligro la ciberseguridad de un sistema de información o la información que el sistema procesa, almacena o transmite; o **ii)** infringe las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable, sea o no producto de una actividad maliciosa.

Comunicación A- 7266 BCRA - 16/04/2021:

Investigación de Ciberincidentes y Preservación de Evidencias:

2.2.6. Capacidades y registros para la investigación: El desarrollo de una adecuada gestión de **"logs",** comprende herramientas para **recopilar y almacenar registros del sistema que serán necesarios para la investigación y el análisis de incidentes**. Los tipos de "logs" o registros que se recopilan y el período de retención deben definirse con anterioridad, en función a la clasificación de la información, de las normas y regulaciones vigentes. **Las capacidades técnicas y forenses son necesarias para preservar la evidencia y analizar fallas de control, identificar problemas de seguridad y otras causas relacionadas con un ciberincidente**. En caso de no contar con capacidades propias, se puede contratar un servicio de terceros. Es necesario que el personal que realiza el trabajo forense esté adecuadamente capacitado y siga procedimientos estandarizados para preservar la integridad de las pruebas, los datos y los sistemas durante las investigaciones.

Comunicación A- 7266 BCRA - 16/04/2021:

2.3.2. Investigación forense y análisis:

2.3.2.1. Para la investigación forense del incidente se requiere contar con **“logs” o registros de auditoría de los sistemas y de los dispositivos**. Analizar las alertas, indicadores (de seguridad y sistemas), investigar y correlacionar eventos posibilitará al equipo de respuesta determinar el impacto de un incidente y posiblemente identificar el origen. Para la respuesta, también se recuperan datos de los dispositivos informáticos involucrados en la interacción como los conectados a la red, procesos en ejecución, sesiones de usuarios, archivos abiertos, de los equipos relevantes sus configuraciones y contenidos de memoria, entre otros. La integridad de dichos datos debe asegurarse para un adecuado análisis.

2.3.2.2. Al momento de una investigación forense será importante que los sistemas de donde se obtengan los registros de sistemas se encuentren sincronizados.

2.3.2.3. Se recomienda contar con diversas fuentes de información tanto internas como externas para una evaluación rápida de las amenazas y de las causas de un ciberincidente.

Comunicación A- 7266 BCRA - 16/04/2021:

2.5.5. Registro de actividades: Se deben **documentar y registrar**, en la medida de lo posible, todas las acciones encaradas **desde el momento en que se detectó el incidente, hasta su resolución final, para posibilitar su seguimiento**. Recuperadas las operaciones, los registros facilitarán poder revertir las acciones tomadas hasta restablecer las condiciones previas al incidente o solucionar problemas en caso de que las acciones de recuperación no tengan éxito. Será necesario registrar las herramientas y los artefactos, tales como “scripts”, cambios de configuración entre otros, utilizados en la restauración y recuperación para un futuro uso o para la mejora de procesos y/o sistemas actuales.

2.6.2. Notificación de ciberincidentes:

2.6.2.1 Se debe **reportar la información relevante de ciberincidentes a las autoridades según lo requieran** y de acuerdo con los plazos establecidos por los marcos normativos correspondientes. Para respaldar la notificación efectiva y oportuna de ciberincidentes, tienen que desarrollar pautas internas sobre cuándo y a quién se debe informar los diferentes tipos de incidentes. Para mejorar la comprensión, se puede contar con ejemplos de diferentes tipos de incidentes y de informes.

Comunicación A- 6492 BCRA – 20/03/2020: Emergencia Sanitaria por COVID 19_

2.1 Continuar prestando los servicios que usualmente prestan en forma remota, como ser: constitución de plazos fijos, otorgamiento de financiaciones y los servicios relacionados con el sistema de pago.

Comunicación A – 6684 BCRA – 23/04/2019:

6.4. Escenarios de Canales Electrónicos:

- **Credenciales y Medios de Pago (CM)**: Elementos para la identificación, autenticación y autorización de acceso/uso de los medios y dispositivos de los Canales Electrónicos. Se incluyen elementos físicos y lógicos que funcionan como mecanismos de consumo, sustitutos del efectivo, que permiten generar transacciones financieras de débito o crédito en las cuentas de los clientes.

- **Dispositivo/Aplicación (DA)**: Son los dispositivos y piezas físicas y lógicas intervinientes en la operación de los Canales Electrónicos.

- **Transacciones (TR)**: Operaciones financieras, operativas y de consulta que permita realizar el Canal Electrónico, con requisitos técnico-operativos mínimos particulares.

Log Transaccional Servicios

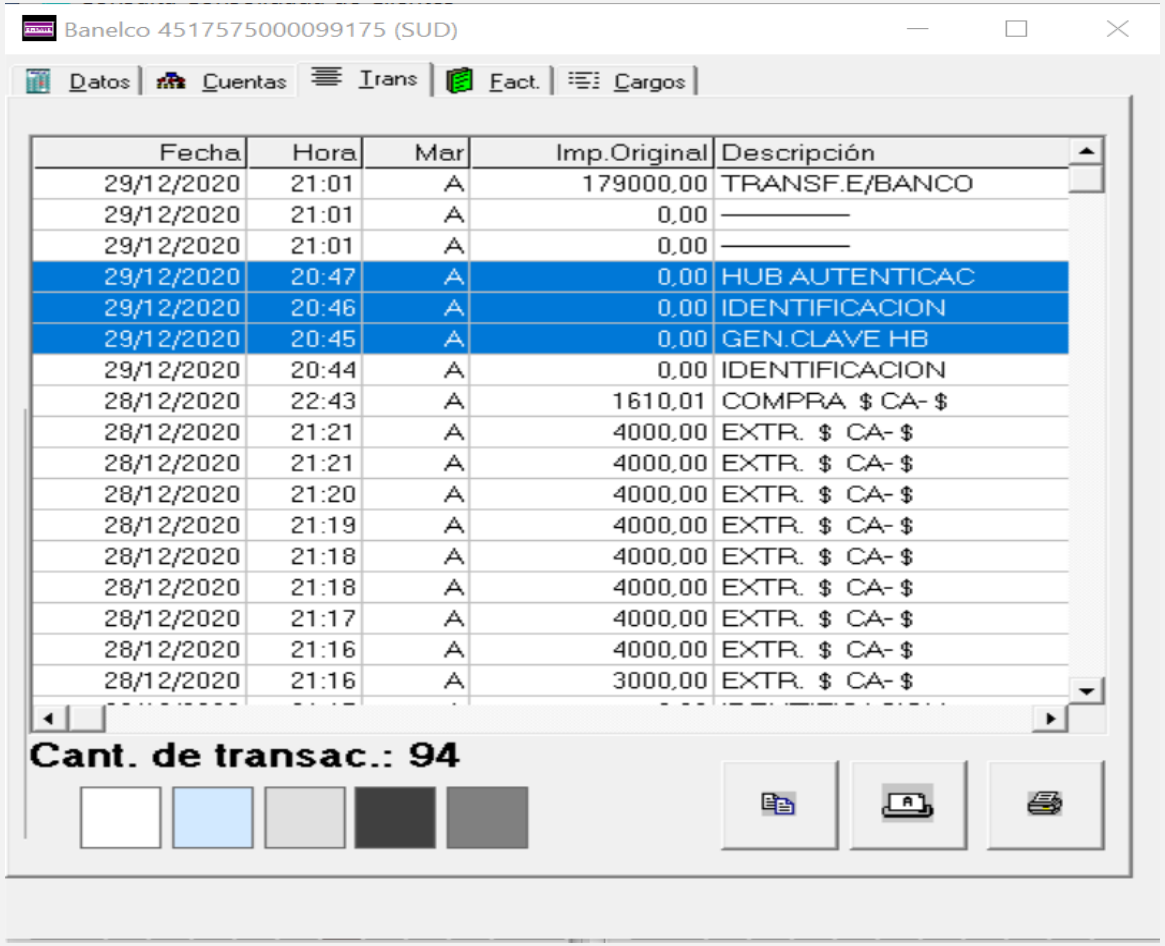
Persona	Usuario Ebank	IP Acceso - IMEI - UniqueID	Fecha Hora	Fecha	Hora Fraccion 60min	Tipo Canal	Canal	Tipo Evento Canal	Grupo Evento Canal
CU 0801220288395382	20288395382	000000000000000023d6827848ace69	29/12/2020 21:01	29/12/2020	21	MOBILE	MB	ConsultaBonosYAcciones	CONSULTAS / SERVICIOS
CU 0801220288395382	20288395382	000000000000000023d6827848ace69	29/12/2020 21:01	29/12/2020	21	MOBILE	MB	ConsultaCotizacionMonedaExtranjera	CONSULTAS / SERVICIOS
CU 0801220288395382	20288395382	000000000000000023d6827848ace69	29/12/2020 21:01	29/12/2020	21	MOBILE	MB	ConsultaFondos	CONSULTAS / SERVICIOS
CU 0801220288395382	20288395382	000000000000000023d6827848ace69	29/12/2020 21:01	29/12/2020	21	MOBILE	MB	Transferir Con Cuenta	TRANSFERENCIAS
CU 0801220288395382	28839538	000000000000000023d6827848ace69	29/12/2020 21:01	29/12/2020	21	MOBILE	MB	Validar Token Virtual	CONSULTAS / SERVICIOS
CU 0801220288395382	20288395382	000000000000000023d6827848ace69	29/12/2020 21:01	29/12/2020	21	MOBILE	MB	Consulta Tarjeta Coordenadas Banco	CONSULTAS / SERVICIOS
CU 0801220288395382	20288395382	000000000000000023d6827848ace69	29/12/2020 21:01	29/12/2020	21	MOBILE	MB	Validar CBU	CONSULTAS / SERVICIOS
CU 0801220288395382	20288395382		29/12/2020 20:53	29/12/2020	20	E-BANK PATAGONIA	EB	insertLoan	CONSULTAS / SERVICIOS

Consulta Transacciones BANELCO

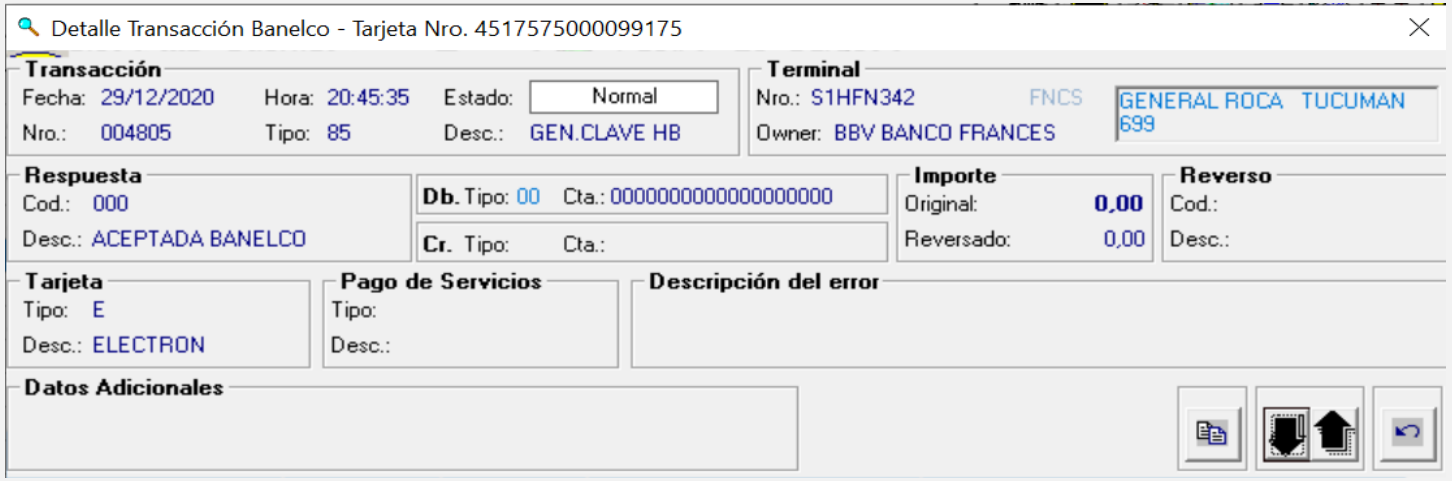
Tarjeta Débito (TD): 4518501009817 6

Fecha	Hora	Mar	Imp.Original	Descripción	Transaccion	Desc. Resp	Cod.Rev.	Terminal
29/12/2020	21:01	A	179000	TRANSF.E/BANCO	528645	ACEPTADA		TISD0000
29/12/2020	21:01	A	0	----------	952044	ACEPTADA		TISD0000
29/12/2020	21:01	A	0	----------	606843	ACEPTADA		TISD0000
29/12/2020	20:47	A	0	HUB AUTENTICAC	4808	ACEPTADA		S1HFN342
29/12/2020	20:46	A	0	IDENTIFICACION	4806	ACEPTADA		S1HFN342
29/12/2020	20:45	A	0	GEN.CLAVE HB	4805	ACEPTADA		S1HFN342
29/12/2020	20:44	A	0	IDENTIFICACION	4803	ACEPTADA		S1HFN342
28/12/2020	22:43	A	1610,01	COMPRA $ CA- $	840830	ACEPTADA		98835703
28/12/2020	21:21	A	4000	EXTR. $ CA- $	1275	ACEPTADA		S1CSD193
28/12/2020	21:21	A	4000	EXTR. $ CA- $	1274	ACEPTADA		S1CSD193

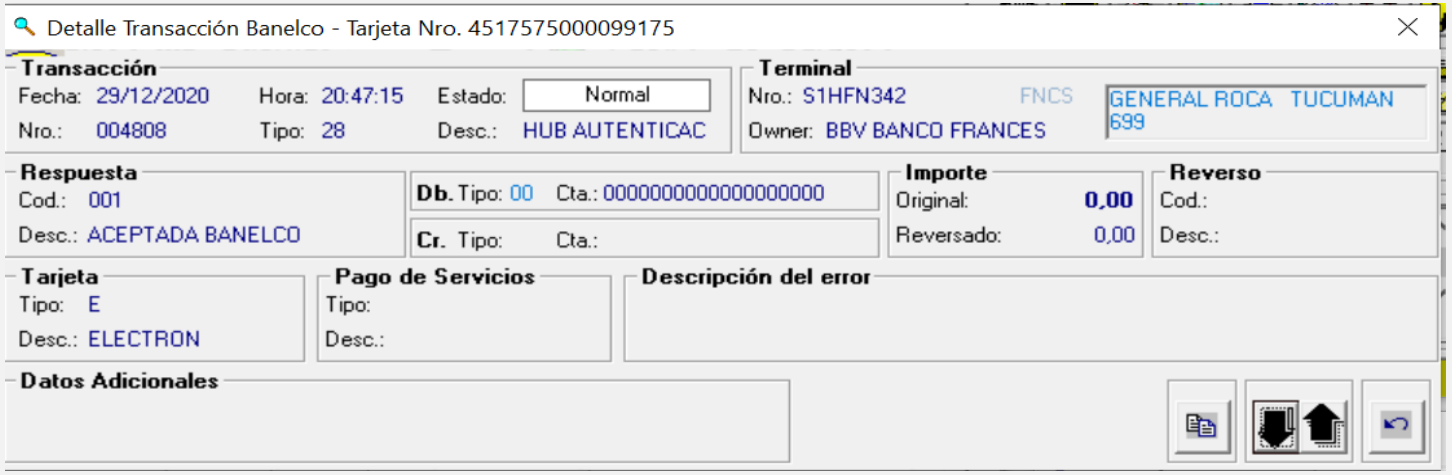
Movimientos con TD: generación de claves Token y Home Banking



Generación Clave Home Banking



Generación Clave Token

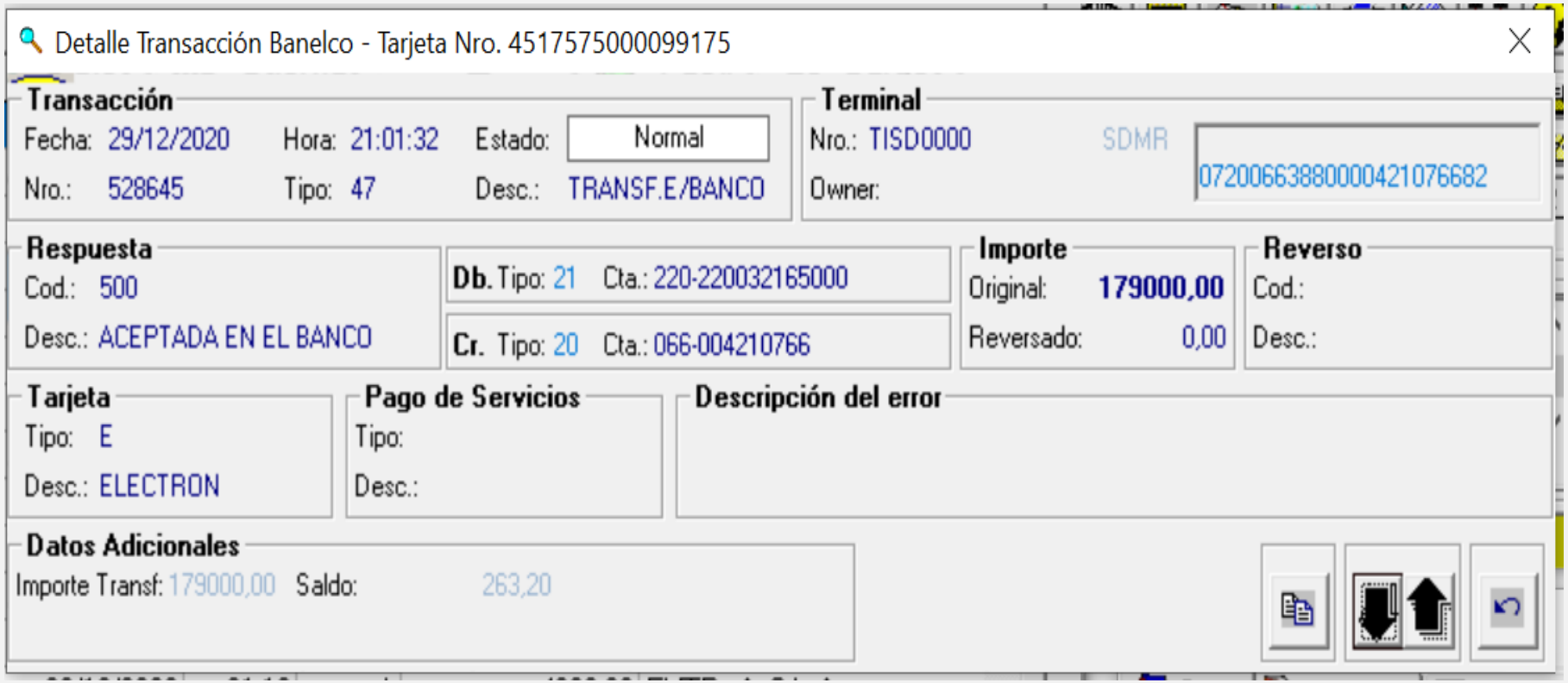


Préstamo tomado por Mobile con IMEI/ID único n°000000000

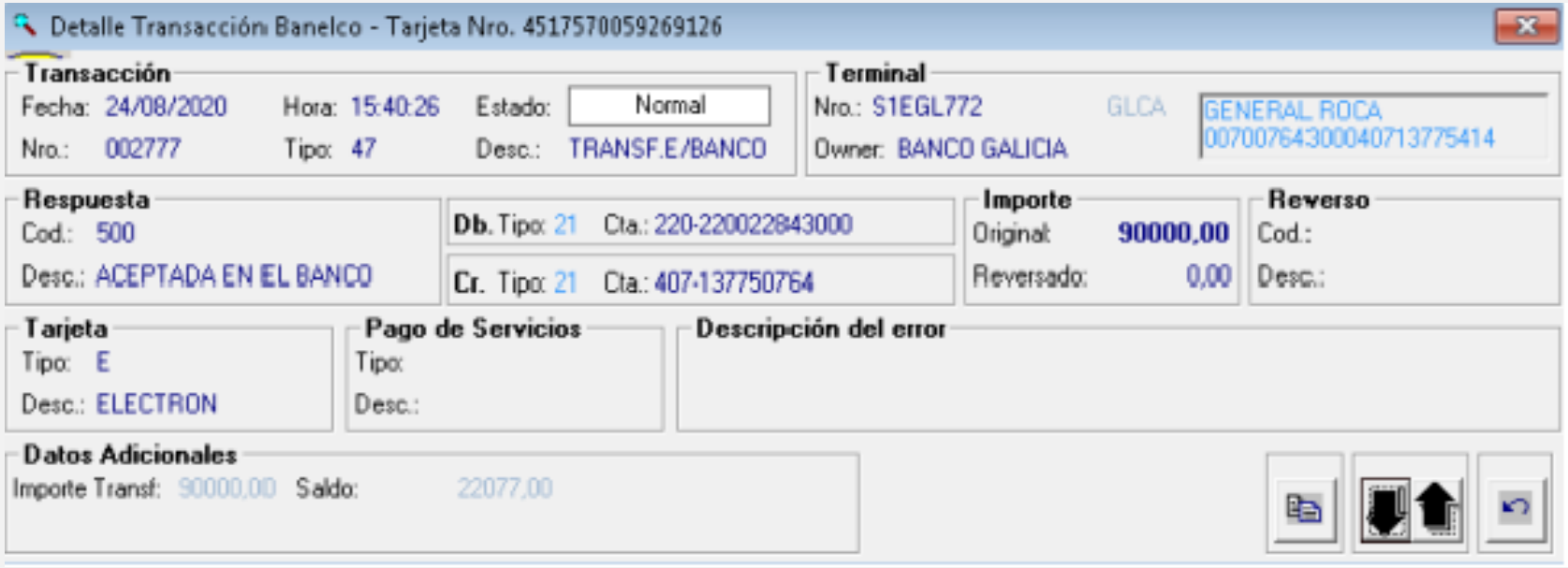
Sucursal 10 Módulo 354 Transacción 410 Relación 73 Caja 0
Contabilizado 29/12/20 Hora 20:53:28 F. valor contable 29/12/20
INGRESO Usuario USRNSBT Workstation PKPR0549
CONFIRMACION Usuario USRNSBT Workstation PKPR0549
Textos

Suc	C.Contable	Mda.	Esp.	Cuenta	Operación	Sop	DH	Importe
220	131731024	80	0	220032165	6354251	0	Db	180.800,00
220	831715336	80	0	220032165	6354251	0	Db	180.800,00
220	931715336	80	0	0	0	0	Cr	180.800,00
220	321155316	80	0	220032165	6354251	0	Cr	1.356,00
220	321155116	80	0	220032165	6354251	0	Cr	180,80
220	311726004	80	0	220032165	0	0	Cr	179.263,20

Transferencia por Mobile –IMEI- y validación de Clave Token



Transferencia Realizada por Cajero Automático (ATM)



DEBIN: Débito Inmediato (Comunicación A-6099 BCRA)

Consulta DEBIN

Desde Hasta

Órdenes de DEBIN recibidas | 01/03/2021 | 22/09/2021 | BUSCAR

Fecha de vencimiento	Originante	Destinatario	Importe	Estado	
13/03/2021	Sofia GACHON	SOTO, MARCELO DAMIAN	97.000,00	Acreditado	>

DEBIN – Datos del Débito Inmediato

Datos de la operación

Id del Debin:	Z86VRPQ2GLR1P1L9GLY0M1
Estado	0600 - ACREDITADO
Fecha y Hora	18/06/2021 - 19:20
Importe	$100.000,00
Concepto	Varios

Datos del Vendedor

Titular

CUIT / CUIL / CDI	20-33695563-8
CBU	0000003100032637413748

Datos del Comprador

Titular

CUIT / CUIL / CDI	27-34128776-1
CBU	0340220908220035337001

Algunas cuestiones de la problemática actual:

- Divulgación de claves/datos personales a terceros.
- Préstamos personales pre aprobados desproporcionados al perfil patrimonial del cliente.
- Sistemas tecnológicos o seguridad insuficientes para neutralizar nuevas modalidades de posibles fraudes.
- Necesidad de incorporar nuevos elementos de identificación positiva y posibilidad de arrepentimiento de la transacción.
- Falta de capacitación o conocimiento de los clientes sobre los riesgos y las medidas de seguridad para operar en canales electrónicos.
- Clientes hipervulnerables.
- Dificultades para desbaratar el fraude y sus responsables: Necesidad de coordinar y colaborar acciones con investigación penal.
- Carencia de cobertura para este tipo de riesgo –fraude-.

MUCHAS GRACIAS

Dr. Jorge Arturo Gómez