**Buenos Aires, 30 de marzo del 2022**

**Asociación de Bancos Públicos y Privados**

**De la República Argentina**

**ABAPPRA**

**Lic. Eduardo Hecker**

**Presidente**

**S / D**

De nuestra consideración:

Las Asociaciones de Usuarios y Consumidores de la República Argentina, abajo firmantes, queremos plantear nuestra disconformidad y rechazo de la campaña de publicidad denominada *“Las Claves No se Comparten”[[1]](#footnote-1)* implementada por ABAPPRA *“…para la prevención de las estafas virtuales”*, ya que la misma **resulta falaz y denigrante para los usuarios que fueron engañados a través de estafas virtuales, ya que se pretende hacer recaer la responsabilidad de las ciberestafas sufridas por los propios usuarios perjudicados al usar, servicios de banca electrónica y banca móvil, ofrecidos por entidades que no implementaron eficientemente las disposiciones de control vigentes.**

La campaña *“Las Claves No se Comparten”* consiste en la difusión en los medios de comunicación social de dos spots publicitarios – informativos, seguidos de varios spots de apoyo protagonizados por varios artistas y periodistas que difunden  **consejos de seguridad que es bueno que el usuario conozca**, **como por ejemplo: no publicar información personal en redes sociales, precaución ante llamadas sospechosas de presuntos representantes de bancos, uso de contraseñas fuertes, operar con cuentas verificadas, bloquear mensajes de procedencia dudosa, etc.**

Pero, debemos resaltar que en el spot más representativo de *“Las Claves No se Comparten”,* una simpática y perspicaz joven (“Clara”) al recibir un WhatsApp supuestamente de su banco se da cuenta que se trata de un intento de estafa (phising) y rápidamente desiste de entrar al link incluido en el mensaje y corta la comunicación. *“****Clara la tiene clara”* expresa el mensaje publicitario.**

**Este aviso marca claramente que el eje central de la campaña promovida por ABAPPRA es que las ciberestafas se producen por culpa de los usuarios quienes comparten irresponsablemente sus claves con terceros**. Este argumento es utilizado desde hace años por las entidades bancarias para des responsabilizarse de las ciberestafas y desentenderse de los perjuicios económicos que ocasionan, a sus propios clientes, con su accionar negligente.

Las entidades bancarias argentinas toleraron durante años, en cómplice silencio, que sus clientes sufrieran estafas virtuales a través del sistema de préstamos online. Pese a las miles de denuncias y reclamos, no hicieron nada *motu proprio* para corregir esta situación que era de conocimiento público y notorio, como lo reflejo la prensa durante años. Cabe mencionar que pese a que estos préstamos eran legalmente nulos, por carecer el contrato uno de sus elementos constitutivos y esenciales como es el consentimiento y la voluntad de contratar y tomar el crédito, las entidades bancarias impertérritas continuaron cobrando y exigiendo los pagos de los créditos fraudulentos. Fue necesaria la intervención del regulador (BCRA) a través de la Comunicación A 7319 del 01/07/2021 y Comunicación A 7370 del 24/09/2021 para que los bancos tomaran acciones para incrementar el nivel de seguridad y requerir un mayor grado de validación de la identidad del usuario.

Es importante comentar que ya existían, antes de estas disposiciones, una serie de medidas de seguridad requeridas por el BCRA cuya aplicación estricta hubieran evitado gran número de estafas virtuales, quizás la más fundante en la norma por la Comunicación A 5230 de fecha 26/09/2011 sobre medidas de precaución en las transferencias inmediatas de fondos la cual establecía una serie de recaudos cuyo fiel cumplimiento habría evitado gran número de fraudes, cito: *“En función de la política “Conozca a su cliente”* ***se recomienda que, de manera previa a la efectivización de una transferencia, se tomen recaudos especiales, específicamente sobre esta operatoria, a los fines de continuar con la política de minimizar el riesgo de fraude informático*** *particularmente respecto a las cuentas que presenten las siguientes características: Cuentas de destino que no hayan sido previamente asociadas por el originante de la transferencia a través de cajeros automáticos, en sede de la entidad financiera o por cualquier otro mecanismo que las entidades financieras consideren pertinente; 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. Por otra parte, dentro del marco de seguridad establecido oportunamente,* ***se recomienda habilitar mecanismos para fortalecer la autenticación de ordenantes y receptores, y el seguimiento de las transacciones de forma que permitan detectar alteraciones de la identidad y comportamientos inusuales de las operaciones cursadas…****”*

También podemos mencionar la Comunicación A 5374 de fecha 12/12/2012 sobre requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras, en donde se establece que: *“Control de Acceso. Las entidades deben adquirir, desarrollar y/o adecuar los mecanismos implementados para la* ***verificación de la identidad y privilegios 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.”*

Pero la falta de un accionar proactivo por parte de las entidades bancarias no se limita a los hechos mencionados *ut supra*. **Son crónicos los reclamos de usuarios financieros a los que se les efectúan débitos no autorizados a sus cajas de ahorro mediante el sistema de código de descuento y débitos automáticos por parte de terceras entidades, cuando no créditos de dinero totalmente desconocidos por los usuarios**. Las entidades bancarias no realizan por sí mismas la más mínima averiguación previa para cerciorarse que estos débitos en concepto de “seguros” y/o de diversos servicios (de dudosa utilidad) fueron efectivamente autorizados por el usuario financiero. Esta práctica se ampara en la pésima redacción de la norma[[2]](#footnote-2) que regula las Cuentas Sueldo y Cajas de Ahorro. Son los jubilados y pensionados, usuarios hipervulnerables por definición, los principales blancos de éstas prácticas quienes ven sus magras jubilaciones desangrarse durante años mediante éstas prácticas delictivas de robo hormiga. Sin embargo, la industria bancaria nada hace al respecto, cuando no puede desconocer que esto ocurre a diario.

Afortunadamente la Justicia Nacional ha comenzado a poner las cosas en su lugar fallando en contra de las entidades bancarias en casos de estafas virtuales. (Como en los fallos: “SUAREZ DANIEL RICARDO C/ BANCO DE LA PROVINCIA DE BUENOS AIRES S/ NULIDAD DE CONTRATO”; “URQUÍA, NICOLÁS MARTÍN C/ BANCO BBVA ARGENTINA S.A. – ABREVIADO”; “SANCHEZ MAXIMILIANO JAVIER C/ BBVA BANCO FRANCES SA S/ MATERIA A CATEGORIZAR”) No puede ser de otra forma ya que es pacífica la jurisprudencia y doctrina que establece que la relación jurídica que vincula al usuarios financiero con una entidad bancaria es una relación de consumo, según lo establecido por el artículo 3° de la Ley N° 24.240 y artículo 1.092° del Código Civil y Comercial de la Nación, estando alcanzada por el marco jurídico protectorio establecido en el artículo 42 de nuestra Constitución Nacional, por la Ley N° 24.240; Ley provincial N° 13.133 Código Provincial para la Implementación de los Derechos de los Consumidores y Usuarios, así como las normas de protección de derechos de usuarios financieros del BCRA. Existiendo, además, en cabeza de los sujetos obligados –bancos– una responsabilidad de tipo objetiva en lo referente a la seguridad que deben ofrecer a sus clientes en el cuidado de los valores puestos bajo su custodia (artículo 40 de la Ley N° 24.240) y que dicha responsabilidad se hace extensiva a las operaciones de banca electrónica y banca móvil puestas a disposición de los usuarios financieros, debiendo las operaciones realizadas por estos canales ser totalmente seguras e invulnerables al accionar delictivo

También resulta pertinente mencionar que las entidades bancarias jamás ofrecieron ningún tipo de apoyo o contención a las víctimas, lejos de ello, se limitaron a exigir el riguroso pago de las cuotas de los créditos fraudulentos sin dar explicaciones y haciendo oídos sordos a los reclamos de sus clientes. **Solo merced al accionar de distintos entes públicos como la Dirección Nacional de Defensa del Consumidor o la Defensoría del Pueblo, como así también las asociaciones de usuarios y consumidores, al trabajo del periodismo al divulgar los hechos, y a las presentaciones judiciales**, **solo así se comenzó a conseguir que las entidades bancarias respondan y asuman el costo económico de su responsabilidad frente a sus clientes estafados buscando acuerdos conciliatorios con las víctimas, a la vez que se lograba que el regulador (BCRA) incremente los requerimientos de seguridad informática**.

Corresponde al regulador (BCRA) diseñar e implementar normativas para que las entidades financieras cumplan con lo establecido en las Directrices para la Protección del Consumidor de Naciones Unidas (UNCTAD/DITC/CPLP/MISC/2016/1) [[3]](#footnote-3), entre ellas la directriz “J” la cual exige a los Estados a implementar normativas que ofrezcan a los consumidores: *“Un grado de protección para los consumidores que recurran al comercio electrónico que no sea inferior al otorgado en otras formas de comercio.”* Se expresa en un mismo sentido el apartado 66 de este instrumento internacional al establer: *a) Políticas para la regulación y la aplicación efectiva de las normas en el ámbito de la protección del consumidor de servicios financieros; c) Controles y mecanismos de seguros adecuados para proteger los activos de los consumidores, incluidos los depósitos; f) La actuación responsable de los proveedores de servicios financieros y sus agentes autorizados, en particular en lo que respecta a la concesión responsable de préstamos y la venta de productos que se ajusten a las necesidades y los medios del consumidor; g) Controles apropiados para proteger los datos financieros del consumidor contra el fraude y el abuso, entre otros. Apartado 67: Los Estados Miembros deben adoptar medidas para reforzar e integrar las políticas de los consumidores relativas a la inclusión financiera, la educación financiera y* ***la protección de los consumidores en cuanto al acceso y la utilización de servicios financieros.***

Ya en el año 2012 el Banco Mundial publico una Guía de Buenas Prácticas para la Protección al Consumidor Financiero[[4]](#footnote-4). En el capítulo dedicado a la Banca por Internet y Banca por Teléfono Móvil recomendaba que: *“a) La prestación de servicios de banca por Internet y a través de teléfonos móviles debería estar soportada por un sólido marco legal y regulatorio; b) Los reguladores deberían asegurar que los bancos o proveedores de servicios financieros que ofrecen banca por Internet y banca móvil tengan establecido un programa de seguridad que garantice: i. la privacidad, confidencialidad e integridad de los datos; ii. la autentificación, la identificación de las contrapartes y el control de acceso; c) Los bancos también deberían implementar un programa de supervisión para monitorear las condiciones de control y el rendimiento de terceros, especialmente cuando los agentes se utilizan para llevar a cabo la banca móvil. Y queremos destacar el punto e):* ***Deberían existir reglas claras sobre los procedimientos para la resolución de errores y fraudes.****”*

Por su parte, el Informe de Riesgos Globales 2022 del Foro Económico Mundial menciona que: *“… las amenazas a la ciberseguridad están creciendo (en 2020, los ataques de malware y ransomware aumentaron un 358 % y un 435 % respectivamente) y están superando la capacidad de las sociedades para prevenirlos o responder a ellos de manera efectiva. Las barreras de entrada más bajas para los actores de ciberamenazas, los métodos de ataque más agresivos, la escasez de profesionales de ciberseguridad y los mecanismos de gobernanza fragmentados están agravando el riesgo. (…) Los riesgos intangibles, como la desinformación,* ***el fraude y la falta de seguridad digital, también afectarán la confianza pública en los sistemas digitales****.”[[5]](#footnote-5)*

Ni la banca electrónica, ni la banca móvil, ni el comercio electrónico dejarán de incrementarse. Vinieron para quedarse definitivamente. La actividad económica que se despliega sobre estas plataformas digitales continuará creciendo, así como su participación en la actividad económica nacional y mundial, y las ganancias también irán en aumento, en tanto y en cuanto operar de esta forma resulte seguro para los consumidores. Del mismo modo, el accionar delictivo que opera sobre estas plataformas no dejará de actuar y de encontrar nuevas formas de realizar fraudes y ciberestafas. Es por ello que urge a las partes involucradas –la industria bancaria y el regulador– a actuar en consecuencia con seriedad y decisión, realizando las inversiones que resulten necesarias para garantizar la seguridad de las operaciones de banca electrónica y móvil. La Republica Argentina cuenta con el talento y los recursos humanos y materiales para enfrentar con éxito esta tarea. Solo falta la decisión de las entidades bancarias de invertir recursos en mejorar la seguridad informática de los servicios que ofrece a los usuarios financieros.

Los usuarios financieros –sus prácticas y conocimientos en materia de seguridad– son el eslabón más débil del sistema y dicho sistema tiene que contemplar este hecho y diseñar los mecanismos necesarios que contemplen esta realidad empírica. Existe una asimetría abismal entre la responsabilidad que le cabe a un usuario y la que le corresponde a un banco. Asimetría en materia de información, recursos, capacidades y obligaciones legales. No pretendan hacer recaer la responsabilidad del resguardo de los valores en los hombros de los usuarios. Los bancos cobran comisiones para efectuar esta tarea. A los efectos prácticos y legales, los bancos tienen la misma responsabilidad en caso de un ciberfraude que sufra uno de sus clientes, como si la bóveda del banco fuera penetrada y vaciada por boqueteros. Existe un claro deber de seguridad en cabeza de los sujetos obligados –bancos– para que se refuerce la seguridad en todos los canales electrónicos disponibles: ATMs (cajeros automáticos), TAS (terminales autoservicio), banca de internet (BI) y banca móvil (BM).

La única forma de evitar las ciberestafas es el compromiso de la industria y la inversión de recursos humanos y materiales. Por empezar, el fiel cumplimiento de los requisitos técnico-operativos de monitoreo y control de seguridad informática solicitados por el BCRA a través de las Comunicaciones 6017, 7153, y 7370, a saber:

* Comunicación A 6017/2016:
* RMC003: Debe realizarse el seguimiento sobre los CE de los cambios de configuración de seguridad y verificar los niveles de actualización de: sistemas operativos, bases de datos, vínculos de comunicación, herramientas que previenen y detectan la presencia de código malicioso, equipamiento de seguridad de red, controladores de tráfico y cualquier otra herramienta de seguridad. Deben incluir, sin limitarse a:

a. Seguimiento de privilegios y derechos de acceso.

b. Procesos de copia, resguardo y recuperación de información.

c. Disponibilidad de los dispositivos del CE.

d. Alarmas, alertas y problemas detectados por los sistemas de registro de eventos.

* RMC004: Las entidades deben disponer de mecanismos de monitoreo transaccional en sus CE, que operen basados en características del perfil y patrón transaccional del cliente bancario, de forma que advierta y actúe oportunamente ante situaciones sospechosas en al menos uno de los siguientes modelos de acción:

a. Preventivo. Detectando y disparando acciones de comunicación con el cliente por otras vías antes de confirmar operaciones.

b. Reactivo. Detectando y disparando acciones de comunicación con el cliente en forma posterior a la confirmación de operaciones sospechosas.

c. Asumido. Detectando y asumiendo la devolución de las sumas involucradas ante los reclamos del cliente por desconocimiento de transacciones efectuadas.

* Comunicación A 7153/2020:
* 2.3.2.6. Establecer reglas para el manejo de las devoluciones y situaciones donde exista una sospecha de fraude.
* 2.3.3.5. Utilizar herramientas de mitigación de fraude que permitan identificar patrones sospechosos, y alertar a los usuarios
* 1.3.4. Autorización. Aprobar o denegar una instrucción de pago válida remitida por un cliente ordenante a una entidad originante o Proveedor de Servicios de Pago que ofrece cuentas de pago, en base a criterios tales como la disponibilidad de saldos suficientes o la sospecha de fraude.
* 2.6. Herramientas de mitigación de fraude: cada esquema de transferencias inmediatas contará con herramientas de mitigación de fraude que permitan identificar patrones sospechosos, y alertar a los usuarios antes o después de la autorización de la transacción. Cuando se deniegue una transferencia al momento

de la autorización por esta causa, se deberá informar al usuario que se debe a una sospecha de fraude.

* Comunicación A 7319/2021:
* Requisito RMC011: El monitoreo transaccional en los CE debe basarse, pero no limitarse a lo siguiente:

a) La clasificación de ordenantes y receptores en base a características de su cuenta y transacciones habituales, incluyendo pero no limitándose a frecuencia de transacciones por tipo, monto de transacciones y saldos habituales de cuentas.

b) Determinación de umbrales, patrones y alertas dinámicas en base al comportamiento transaccional de ordenantes y receptores según su clasificación.

* Comunicación A 7370/2021:
* RMC012: Para la autorización de un crédito preaprobado la entidad debe verificar fehacientemente la identidad de la persona usuaria de servicios financieros involucrada. Esta verificación debe hacerse mediante técnicas de identificación positiva, de acuerdo con la definición prevista en el glosario y en el requisito técnico operativo específico (RCA040) de estas normas. Asimismo, se deberá constatar previamente a través del resultado 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. Una vez verificada la identidad de la persona usuaria, la entidad deberá comunicarle –a través de algunos de los puntos de contacto disponibles– que el crédito se encuentra aprobado y que, de no mediar objeciones, el monto será acreditado en su cuenta a partir de los 2 (dos) días hábiles siguientes. El citado plazo de acreditación podrá ser reducido en el caso de recibirse la conformidad del usuario de servicios financieros de manera fehaciente.

La entidad financiera quedará exceptuada de implementar lo previsto precedentemente, en la medida de que dé cumplimiento a alguna de las siguientes condiciones:

a. Que para la autorización de un crédito preaprobado la entidad financiera verifique fehacientemente la identidad de la persona usuaria de servicios financieros involucrada, mediante soluciones biométricas con prueba de vida.

b. Que la entidad financiera cancele el crédito preaprobado, asuma la devolución de las sumas involucradas y anule los posibles efectos sobre la situación crediticia

de la persona usuaria de servicios financieros afectada, ante la denuncia policial presentada por esta persona usuaria de acuerdo con el modelo de acción “asumido” definido en el requisito RMC004, siempre que la denuncia se presente en un plazo máximo de 90 (noventa) días corridos desde el vencimiento de la primera cuota del crédito.

En ambos casos, el crédito solicitado podrá acreditarse de manera inmediata en la cuenta del usuario. La actividad que se realice para el cumplimiento de este requisito debe ser trazable y auditable.

El siguiente es un listado de las acciones que resultan necesarias para verdaderamente prevenir las ciberestafas a los usuarios de servicios financieros. Estas acciones requieren de una inversión de recursos y tal obligación se encuentra en cabeza de los sujetos obligados, los bancos, y no de sus clientes:

* Garantizar niveles de ciberseguridad que cumplan con la norma internacional ISO / IEC 27001 de seguridad de la información.
* Garantizar la responsabilidad proactiva en el manejo de datos personales de los usuarios financieros clientes de las entidades bancarias.
* Diseñar y distribuir gratuitamente a sus clientes software y/o suite de seguridad para operar con la entidad bancaria, poseyendo la capacidad de detectar y eliminar virus o malware presentes en los dispositivos de los usuarios.[[6]](#footnote-6)
* Implementación de un servicio de atención específico para casos de ciberdelitos que funcione 24/7 atendidos por personal idóneo y capacitado, así como la creación de los protocolos de actuación adecuados.
* Implementar mecanismos de aviso de débitos y operaciones en la cuenta en tiempo real, diferimiento de transferencias sospechosas y posibilidad de reversión inmediata de pago en caso de denuncia de ciberestafa.
* Informar el monto anual de inversión en seguridad informática.
* Informar al BCRA y al público en general los casos de estafas virtuales que sufran sus respectivos clientes, detallando intentos de fraude, fraudes concretados y fraudes resueltos.
* Creación de una mesa de trabajo permanente para el intercambio de información y colaboración en materia antifraude entre los integrantes de la actividad bancaria, fuerzas de seguridad, el regulador (BCRA) y la Justicia.
* Implementación en cada entidad bancaria de Centros de Fusión de Fraude Cibernético en donde se integre las diversas áreas involucradas en prevenir y esclarecer los fraudes (informática, prevención de fraudes, seguridad, auditoria interna, jurídicos, etc.) vinculados a los agentes de seguridad estatales y a la Justicia.
* Implementar ciberseguridad adaptativa complementando tecnología con políticas de estrategias de gestión de riesgos de fraude que puedan prevenir, detectar, analizar, responder y recuperar, y seguir evolucionando para poder enfrentar futuras amenazas desconocidas.
* Inversión en monitoreo y detección temprana de manipulación de cajeros automáticos (ATM) para evitar el riesgo de la clonación de tarjetas de débito.

**Todas estas regulaciones, desconocidas para los usuarios, pero de obligado conocimiento, por parte de las entidades financieras, fundamentan claramente nuestra disconformidad y rechazo de la campaña de publicidad denominada** *“Las Claves No se Comparten* implementada por ABAPPRA *“…para la prevención de las estafas virtuales”*, ya que la misma , como hemos fundamentado, **resulta falaz y denigrante para los usuarios que fueron engañados a través de estafas virtuales, pues se pretende hacer recaer la responsabilidad de las ciberestafas sufridas por los usuarios perjudicados al usar servicios de banca electrónica y banca móvil, que fueron ofrecidos por entidades bancarias que no implementaron eficientemente las disposiciones de control vigente.**

**PROTECCIÓN A LOS CONSUMIDORES Y USUARIOS DE LA REPÚBLICA ARGENTINA ASOCIACIÓN CIVIL - PROCURAR (RNAC N°01).**

**ASOCIACIÓN CIVIL DE USUARIOS BANCARIOS ARGENTINOS - ACUBA (RNAC Nº 02).**

**PROTECTORA ASOCIACIÓN DE DEFENSA DEL CONSUMIDOR (RNAC Nº 04).**

**CONSUMIDORES LIBRES COOP LIMITADA DE PROVISIÓN DE SERVICIOS DE ACCIÓN COMUNITARIA (RNAC N° 05).**

**ASOCIACIÓN PROCONSUMER PROTECCIÓN CONSUMIDORES DEL MERCOSUR (RNAC N° 06).**

**ASOCIACIÓN CIVIL POR LOS CONSUMIDORES Y EL MEDIO AMBIENTE ACYMA (RNAC N° 07).**

**ASOCIACIÓN DE CONSUMIDORES Y USUARIOS DE LA ARGENTINA – ACUDA (RNAC N° 08).**

**PREVENCIÓN, ASESORAMIENTO Y DEFENSA DEL CONSUMIDOR - PADEC (RNAC N° 09).**

**USUARIOS Y CONSUMIDORES EN DEFENSA DE SUS DERECHOS (RNAC Nº 10).**

**DEFENSA USUARIOS Y CONSUMIDORES - DEUCO (RNAC Nº 11).**

**COMITÉ DEL CONSUMIDOR –CODELCO- (RNAC N° 12).**

**ASOCIACIÓN CIVIL LIGA DE CONSUMIDORES - LIDECO - (RNAC Nº 13).**

**RED ARGENTINA DE CONSUMIDORES (RNAC Nº 15).**

**CENTRO DE ORIENTACIÓN, DEFENSA Y EDUCACIÓN DEL CONSUMIDOR - CODEC (RNAC Nº 16).**

**ASOCIACIÓN POR LA DEFENSA DE USUARIOS Y CONSUMIDORES - ADUC (RNAC Nº 19).**

**ASOCIACIÓN DE DEFENSA DE DERECHOS DE USUARIOS Y CONSUMIDORES – ADDUC (RNAC Nº 20).**

**ASOCIACIÓN CIVIL DE USUARIOS Y CONSUMIDORES UNIDOS – UCU (RNAC N° 21).**

**ASOCIACIÓN CIVIL CONSUMIDORES EN ACCIÓN (RNAC N° 23).**

**ASOCIACIÓN DE DEFENSA DEL ASEGURADO CONSUMIDORES Y USUARIOS ADACU (RNAC N° 24).**

**CONSUMIDORES ARGENTINOS ASOCIACIÓN PARA LA DEFENSA, EDUCACIÓN E INFORMACIÓN DEL CONSUMIDOR (RNAC Nº 25).**

**ASOCIACIÓN CIVIL CRUZADA CÍVICA PARA LA DEFENSA DE CONSUMIDORES Y USUARIOS DE SERVICIOS PÚBLICOS (RNAC N° 26).**

**ASOCIACIÓN DE DEFENSA DEL CONSUMIDOR DE SANTIAGO DEL ESTERO-ADECSE (RNAC N° 27).**

**ASOCIACIÓN DE CONSUMIDORES Y USUARIOS DE LA ARGENTINA - ADECUA (RNAC N° 28).**

**ASOCIACIÓN COORDINADORA DE USUARIOS, CONSUMIDORES Y CONTRIBUYENTES - ACUCC (RNAC N°29).**

**ASOCIACIÓN DE USUARIOS Y CONSUMIDORES DE LA PROVINCIA DE CORRIENTES - AUC (RNAC N°30).**

**ASOCIACIÓN DE DEFENSA DE CONSUMIDORES ENTRERRIANOS –ADECEN (RNAC N° 33).**

**CONSUMIDORES ALERTA ASOCIACIÓN CIVIL – CONSAL (RNAC N° 36).**

**UNIÓN DE USUARIOS Y CONSUMIDORES (RNAC N°40).**

**FEDERACIÓN DE MUTUALES PARA LA DEFENSA ORGANIZADA DEL CONSUMO - FEMUDECO (RNAC 41).**

**ASOCIACIÓN CIVIL CENTRO DE EDUCACIÓN, SERVICIOS Y ASESORAMIENTO AL CONSUMIDOR – CESYAC (RNAC 42).**

**UNIÓN ARGENTINA PARA LA DEFENSA DEL CONSUMO – UNADEC (RNAC N°44).**

**ASOCIACION CIUDADANA POR LOS DERECHOS HUMANOS-ACDH (RENAC Nº46).**

**ASOCIACIÓN CIVIL CENTRO DE ESTUDIOS PARA LA PROMOCIÓN DE LA IGUALDAD Y LA SOLIDARIDAD –CEPIS- (RNAC N° 47)**

1. <https://www.lasclavesnosecomparten.com.ar/>

   <https://youtu.be/V7oeEu-k-v4>

   <https://youtu.be/hFWwZ1vN2rQ> [↑](#footnote-ref-1)
2. Texto ordenado al 29/10/2021 “Depósitos en Caja de Ahorro, Cuenta Sueldo y Especiales”. Punto 1.10.2. Segunda parte: “*En caso de que el cliente formalice su adhesión al servicio de débito automático a través de la empresa prestadora de servicios, organismo recaudador de impuestos, etc., a fin de efectuar los débitos será suficiente la comunicación que la empresa o ente envíe a la entidad notificando la adhesión, cuya constancia podrá quedar en poder de la empresa o ente.”* [↑](#footnote-ref-2)
3. <https://unctad.org/system/files/official-document/ditccplpmisc2016d1_es.pdf> [↑](#footnote-ref-3)
4. <https://documents1.worldbank.org/curated/ar/447021493843704521/pdf/70157-SPANISH-FinConsumerProtection-GoodPractices-SPANISH-FINAL.pdf> [↑](#footnote-ref-4)
5. <https://www.weforum.org/reports/global-risks-report-2022/in-full/grr2022-executive-summary> [↑](#footnote-ref-5)
6. Acción sugerida en el Informe “Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe 2018” como forma de extender la capa de detección y prevención a la esfera de la interacción

   realizada por los usuarios. (Pág. 150) [↑](#footnote-ref-6)