



BANCO CENTRAL DEL URUGUAY

Montevideo, 17 de junio de 2026

COMUNICACION N°2026/124

Ref: Bancos, Casas Financieras, Cooperativas de Intermediación Financiera, Bancos de Inversión, Instituciones Financieras Externas, Administradoras de Grupos de Ahorro Previo, Casas de Cambio, Empresas Administradoras de Crédito, Entidades Otorgantes de Crédito, Empresas de Servicios Financieros y Empresas Administradoras de Plataformas para Préstamos entre Personas - ARTÍCULO 364.1 DE LA RNRCSF - REQUISITOS PARA DISPOSITIVOS DE CONFIANZA Y AUTENTICACIÓN MEDIANTE PASSKEYS.

Se pone en conocimiento del mercado que la Superintendencia de Servicios Financieros, adoptó con fecha 17 de junio de 2026 la resolución SSF N° 2026-384.

JUAN PEDRO CANTERA

Superintendente de Servicios Financieros

2025-50-1-02303



SUPERINTENDENCIA DE SERVICIOS FINANCIEROS – RESOLUCIÓN

SUPERINTENDENCIA DE SERVICIOS FINANCIEROS

VISTO: Las disposiciones contenidas en el artículo 364.1 de la Recopilación de Normas de Regulación y Control del Sistema Financiero, en la redacción dada por la Resolución comunicada por la Circular N° 2497 de fecha 28 de enero de 2026.

RESULTANDO:

- I) Que la disposición referida en el VISTO actualizó la normativa relativa a la seguridad de los instrumentos electrónicos, incorporando la obligación de aplicar mecanismos de autenticación reforzada de clientes para determinadas operaciones.
- II) Que el referido artículo 364.1 establece que:
 - a) “Se considerará como factor de posesión los dispositivos de confianza que utilice el cliente, siempre que cumplan con los requisitos de enrolamiento detallados en las instrucciones que se impartirán”.
 - b) “La utilización de passkeys será admitida como un mecanismo válido de autenticación reforzada de clientes, siempre que su implementación cumpla con los requisitos dispuestos en las instrucciones que se impartirán”.

CONSIDERANDO:

- I) Que es necesario impartir las instrucciones que establezcan los principios, requisitos técnicos de enrolamiento y condiciones de seguridad que deben cumplir los dispositivos de confianza para ser considerados factor de posesión, de acuerdo con lo previsto en el artículo 364.1 de la Recopilación de Normas de Regulación y Control del Sistema Financiero.
- II) Que también es necesario impartir las instrucciones que establezcan los estándares técnicos y los requisitos de seguridad para la implementación de passkeys como mecanismo válido de autenticación reforzada de clientes, así como procedimientos para la gestión de su ciclo de vida y revocación.

ATENTO: A lo dispuesto en el literal A) del artículo 38 de la Ley Nro. 16.696 del 30 de marzo de 1995 en la redacción dada por el artículo 694 de la Ley N° 20.446 de 16 de diciembre de 2025 a los informes emitidos por esta Superintendencia de Servicios Financieros y demás antecedentes en expediente 2025-50-1-02303.

EL SUPERINTENDENTE DE SERVICIOS FINANCIEROS

RESUELVE:

- 1. Poner en conocimiento de los Bancos, Casas Financieras, Cooperativas de Intermediación Financiera, Bancos de Inversión, Instituciones Financieras Externas, Administradoras de Grupos de Ahorro Previo, Casas de Cambio,

Empresas Administradoras de Crédito, Entidades Otorgantes de Crédito, Empresas de Servicios Financieros y Empresas Administradoras de Plataformas para Préstamos entre Personas que, a efectos de cumplir con lo dispuesto en el artículo 364.1 de la Recopilación de Normas de Regulación y Control del Sistema Financiero, en la redacción dada por la Resolución comunicada por medio de la Circular 2497 del 28 de enero de 2026, para poder considerar como factor de posesión los dispositivos de confianza que utilice el cliente y admitir la utilización de passkeys como mecanismo válido de autenticación reforzada, deberá cumplirse con las siguientes disposiciones:

1. Definiciones

Dispositivo de confianza: dispositivo físico del cliente que haya sido previamente enrolado por la institución y vinculado de forma segura a su identidad y aceptado expresamente como tal por el cliente.

Passkey: estándar de autenticación basado en criptografía asimétrica en el que la clave pública se guarda en el servidor del servicio y la clave privada se almacena de forma segura en el dispositivo de confianza del cliente.

2. Dispositivos de confianza admisibles como factor de posesión.

Para que un dispositivo de confianza sea considerado como factor de posesión dentro de un proceso de autenticación reforzada, deberá cumplirse con los siguientes principios y requisitos:

2.1 Principios generales

El enrolamiento y uso del dispositivo de confianza deberá ajustarse al cumplimiento íntegro de los siguientes principios:

- a) Vinculación inequívoca entre el cliente y el dispositivo enrolado.
- b) Independencia del factor de posesión respecto de los demás factores utilizados.
- c) Resistencia a suplantación, clonación y uso indebido.
- d) Trazabilidad, registro y auditabilidad del proceso de enrolamiento y de su utilización.
- e) Confianza consentida: el cliente por una acción expresa acepta la confianza en el dispositivo como factor de posesión.
- f) Visibilidad y capacidad de administración por parte del cliente de sus dispositivos de confianza activos, pudiendo en forma simple deshabilitar su uso o suspender como factor de posesión según el tipo de operativa.

2.2 Requisitos del proceso de enrolamiento

Se deberá asegurar en el proceso de enrolamiento de dispositivos de confianza, que:

- a) Se realice únicamente luego de una autenticación reforzada previa del cliente.
- b) Incluya la verificación de la identidad del cliente por un canal con nivel de seguridad equivalente o independiente.
- c) Permita la identificación técnica persistente del dispositivo, utilizando mecanismos criptográficos o tecnológicos que reduzcan el riesgo de duplicación o fraude.
- d) Requiera el consentimiento expreso del cliente, debidamente documentado.
- e) Genere registros suficientes que permitan auditabilidad y aseguren inequívocamente que se cumplió satisfactoriamente.

2.3 Requisitos de seguridad del dispositivo

El dispositivo enrolado como dispositivo de confianza deberá cumplir, como mínimo, con las siguientes condiciones:

- a) Las credenciales, claves o elementos criptográficos asociados al factor de posesión deberán almacenarse en entornos seguros del dispositivo, tales como elementos de hardware o software protegidos, equivalentes Trusted Execution Environment.
- b) Dichos elementos no deberán ser exportables ni reutilizables en otros dispositivos, lo que deberá ser verificado inequívocamente por parte de la Institución considerando los datos de enrolamiento y contexto.
- c) El uso del dispositivo como factor de autenticación deberá encontrarse activo y protegido mediante mecanismos propios del dispositivo, tales como bloqueo por PIN, biometría o contraseña.

2.4 Gestión del ciclo de vida

Se deberá contar con políticas y procedimientos documentados e implementados que contemplen:

- a) La revocación inmediata del dispositivo de confianza ante pérdida, robo, cambio de dispositivo o detección de eventos de seguridad. Dicho extremo se deberá notificar inmediatamente al cliente.
- b) El re-enrolamiento deberá estar sujeto a una nueva autenticación reforzada.
- c) La limitación del número de dispositivos de confianza activos por cliente, de acuerdo con criterios de riesgo.

- d) La revisión periódica de la vigencia de los dispositivos enrolados, previendo la suspensión o inhabilitación de dispositivos cumplido un plazo de no uso, de acuerdo con criterios de riesgo.

3. Uso de passkeys como mecanismo de autenticación reforzada de clientes.

Se admite el uso de passkeys como mecanismo válido de autenticación reforzada de clientes, siempre que se cumpla con los siguientes principios y requisitos:

3.1 Principios de implementación

La utilización de passkeys deberá:

- a) Cumplir con los principios de autenticación multifactor, aun cuando el mecanismo se presente de forma integrada para el cliente.
- b) Respetar el principio de independencia de factores, de conformidad con las buenas prácticas internacionales.

3.2 Estándares técnicos aceptables

Las instituciones deberán implementar passkeys basándose en estándares internacionales ampliamente aceptados y auditables, en particular:

- FIDO2 / WebAuthn y/o CTAP2, conforme a las especificaciones del W3C y de la FIDO Alliance.
- Criptografía de clave pública, con generación y almacenamiento de claves privadas en el dispositivo de confianza del cliente.

No se considerarán aceptables mecanismos propietarios que no permitan verificar adecuadamente el cumplimiento de los requisitos de seguridad.

3.3 Requisitos de seguridad

La implementación de passkeys deberá garantizar que:

- a) Las claves privadas permanezcan exclusivamente en el entorno seguro del dispositivo del cliente.
- b) El mecanismo sea resistente a ataques de phishing, intermediación y reutilización de credenciales.
- c) El uso de la passkey requiera un desbloqueo local del dispositivo, mediante biometría, PIN o contraseña.
- d) Las passkeys se encuentren vinculadas a los servicios y dominios específicos de la institución financiera.

3.4 Revocación

Las instituciones deberán prever mecanismos para la revocación, suspensión o reemplazo de passkeys de forma segura, verificable y auditable.

4. Información al cliente.

Las instituciones deberán brindar a los clientes información clara y suficiente sobre:

- a) Los mecanismos de autenticación utilizados.
- b) Los dispositivos de confianza enrolados y las passkeys activas.
- c) Los procedimientos de revocación.

5. Requisitos de gestión

Las instituciones deberán integrar los requisitos señalados dentro de sus marcos de gestión de riesgos tecnológicos, de seguridad de la información y de control interno, manteniendo la documentación y evidencia necesaria a disposición de la Superintendencia de Servicios Financieros.

- 2. VIGENCIA:** Las instituciones dispondrán para adaptarse a lo dispuesto precedentemente hasta el 1 de enero de 2027.

JUAN PEDRO CANTERA
Superintendente de Servicios Financieros