BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" **7783**	**02/06/2023**

A LAS ENTIDADES FINANCIERAS,
A LAS CÁMARAS ELECTRÓNICAS DE COMPENSACIÓN,
A LAS REDES DE CAJEROS AUTOMÁTICOS,
A LOS PROVEEDORES DE SERVICIOS DE PAGO,
A LAS INFRAESTRUCTURAS DEL MERCADO FINANCIERO:

Ref.: Circular
RUNOR 1-1799:

"Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información". Adecuaciones. "Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información asociados a los servicios financieros digitales." Reglamentación.

Nos dirigimos a Uds. para comunicarles que esta Institución adopto la siguiente resolución:

"1. Aprobar las normas sobre "Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información asociados a los servicios financieros digitales" que constan en anexo y forman parte de la presente comunicación.

2. Derogar la Sección 11. de las normas sobre "Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información".

3. Extender el alcance de las normas sobre "Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información" a las Infraestructuras del Mercado Financiero conocidas como Sistemas de Pago de importancia sistémica: INTERBANKING, COELSA, LINK y PRISMA.

4. Dejar sin efecto las normas sobre "Requisitos operativos mínimos del área de sistemas de información (SI) – tecnología informática".

5. Establecer que estas disposiciones entrarán en vigencia a los 180 días corridos contados desde la fecha de su difusión."

Por último, les hacemos llegar las hojas que, en reemplazo de las oportunamente provistas, corresponderá incorporar en las normas sobre "Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información". Asimismo, se recuerda que en la página de esta Institución www.bcra.gob.ar, accediendo a "Sistema Financiero - MARCO LEGAL Y NORMATIVO - Ordenamientos y resúmenes - Textos ordenados de normativa general", se encontrarán las modificaciones realizadas con textos resaltados en caracteres especiales (tachado y negrita).

Saludamos a Uds. atentamente.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

BANCO CENTRAL DE LA REPÚBLICA ARGENTINA

Mara I. Misto Macias
Gerenta Principal de Normas de Seguridad
de la Información en Entidades

María D. Bossio
Subgerenta General
de Regulación Financiera

ANEXO

B.C.R.A.	TEXTO ORDENADO DE LAS NORMAS SOBRE “REQUISITOS MÍNIMOS PARA LA GESTIÓN DE LOS RIESGOS DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN ASOCIADOS A LOS SERVICIOS FINANCIEROS DIGITALES”

-Índice-

1.1. Sujetos obligados.

1.1.1. Entidades financieras.
1.1.2 PSPs.

1.2. Aspectos generales.

Se denomina servicio financiero digital a toda aquella prestación de servicios financieros a clientes por medios digitales para efectuar al menos, transferencias, pagos, extracciones, consultas u otras operaciones en línea, permitidas por las regulaciones vigentes.

El Directorio o autoridad equivalente del sujeto alcanzado es el responsable primario del establecimiento de estructuras organizacionales, modelos de control y gestión de riesgos relacionados con la provisión de servicios financieros por medios digitales, y de la supervisión de la aplicación de estos, siendo la Alta Gerencia la responsable de su implementación.

En concordancia con lo establecido en las normas sobre “Requisitos mínimos para la gestión y control de los riesgos de la tecnología y seguridad de la información”, los sujetos alcanzados deberán implementar, sumado al conjunto de procesos que dan soporte a las soluciones de servicios financieros provistos a los clientes por medios digitales, una adecuada gestión de:

- La tecnología de la información,
- la seguridad de la información,
- la infraestructura tecnológica y procesamiento,
- del desarrollo, adquisición y mantenimiento de “software”, y
- de la relación con terceras partes.

Para ello, deberán gestionar los riesgos y aplicar medidas de protección y detección sobre las soluciones implementadas, las transacciones realizadas, los dispositivos o medios utilizados y los factores de autenticación durante todo su ciclo de vida para asegurar la integridad, disponibilidad y confidencialidad de la información.

Por otra parte, los sujetos alcanzados deberán establecer procesos de gestión de ciberincidentes y continuidad del negocio que contemplen las disposiciones establecidas en las normas sobre “Requisitos mínimos para la gestión y control de los riesgos de la tecnología y seguridad de la información”, previamente mencionado y en el texto ordenado sobre “Lineamientos para la respuesta y recuperación ante ciberincidentes”.

Las secciones siguientes establecen un conjunto de requisitos mínimos aplicables a los servicios financieros provistos por medios digitales. De acuerdo con los resultados de su gestión de riesgos, los sujetos alcanzados deberán identificar e implementar controles adicionales a los establecidos en esta comunicación.

Los sujetos alcanzados deberán notificar a la Gerencia de Auditoría Externa de Sistemas para su conocimiento, acerca de todos aquellos proyectos que involucren un nuevo producto o tipo de servicio en la provisión de servicios financieros por medios digitales a clientes. Deben informar, como mínimo, 60 días antes de la puesta en producción e incluir las características del producto o servicio, las medidas de protección adoptadas, factores de autenticación utilizados, las actividades de monitoreo previstas, las actividades para la gestión de ciberincidentes, entre otros.

B.C.R.A.	REQUISITOS MÍNIMOS PARA LA GESTIÓN DE LOS RIESGOS DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN ASOCIADOS A LOS SERVICIOS FINANCIEROS DIGITALES
	Sección 2. Gestión de riesgos de los servicios financieros provistos por medios digitales.

Los sujetos alcanzados deberán aplicar principios y prácticas que les permitan identificar, analizar y mitigar los riesgos vinculados con la provisión de servicios financieros por medios digitales, en concordancia con lo establecido en las normas sobre “Requisitos mínimos para la gestión y control de los riesgos de la tecnología y seguridad de la información”.

Los análisis de riesgos deberán considerar, como mínimo, lo siguiente:

a. Los riesgos operacionales, especialmente los relacionados con fraudes internos y a clientes, y los vinculados con tecnología y seguridad de la información.

b. Los riesgos propios de los medios por los cuales se proveen los servicios financieros digitales.

c. Los riesgos vinculados a la apertura de cuenta no presencial de clientes, los factores de autenticación de los clientes y la autorización o confirmación de las instrucciones realizados por los clientes en los servicios digitales.

d. El impacto en los riesgos integrales de la organización.

e. Escenarios que afecten la resiliencia operacional.

3.1. Pautas para considerar en las transacciones financieras digitales.

Los sujetos alcanzados deberán tener debidamente identificados y documentados los servicios digitales brindados y la funcionalidad de cada uno de ellos. Asimismo, deberán diseñar e implementar controles para las transacciones acordes a los resultados de la gestión de riesgos y a la gestión de amenazas y vulnerabilidades. Estos controles deberán ser adaptados en función de los escenarios de monitoreo transaccional definidos. En ese marco, deberán considerar, como mínimo, los siguientes criterios:

a. El cliente deberá estar identificado y autenticado para efectuar cualquier tipo de transacción.

b. Implementar técnicas de autenticación multifactor acordes a los niveles de riesgo, al resultado del monitoreo transaccional y/o cuando superen los umbrales establecidos por la organización.

3.1.1. Confirmación de acciones críticas.

Deberán aplicar técnicas de autenticación multifactor o de identificación digital del cliente, en la confirmación o autorización para la ejecución de al menos, las siguientes acciones críticas:

a. Creación, habilitación y rehabilitación de los factores de autenticación.

b. Suscripción a nuevos productos o servicios, solicitud de créditos preaprobados o aceptación de nuevas condiciones de uso.

c. Cambios de puntos de contactos o de parámetros relacionados con la operación transaccional.

d. Agenda de cuentas de terceros para transferencias.

e. Confirmación de transacciones que se desvíen de patrones predeterminados en los sistemas de monitoreo transaccional.

3.1.2. Confirmación de acciones no críticas.

Para acciones de bajo riesgo, podrán utilizar cuestionarios preconfigurados por el cliente con presentación aleatoria, o el intercambio de código seguro no predecible y de único uso.

3.1.3. Servicios basados en atención telefónicas o plataformas de mensajería.

Cuando, para operar con sus cuentas, se utilicen servicios basados en atención telefónica o plataforma de mensajería, deberán:

a. Habilitar la funcionalidad de acuerdo con los resultados de los análisis de riesgos y la fortaleza de los factores de autenticación.

b. Implementar un registro en tiempo real de toda la información vinculada con la ejecución de transacciones.

c. Evitar la exposición de los factores de autenticación empleados en otros servicios financieros digitales.

d. Efectuar la devolución inmediata de los montos involucrados en caso de desconocimiento por parte del cliente de una transacción realizada por esta vía, pudiendo hacer posteriormente las investigaciones que estimen necesarias.

3.2. Dispositivos y aplicaciones provistos por la organización.

Los sujetos alcanzados deberán diseñar e implementar medidas de seguridad para los dispositivos y/o aplicaciones provistas a los clientes para brindar los servicios financieros digitales que sean acordes a los resultados de la gestión de riesgos y de la gestión de amenazas y vulnerabilidades.

Los dispositivos y aplicaciones provistos por la organización hacen referencia a todo medio digital que se ofrece al cliente para que tenga acceso a los servicios financieros digitales. A modo de ejemplo, entre los dispositivos provistos, se encuentran los cajeros automáticos, las terminales de autoservicios y los kioscos digitales; mientras que, entre las aplicaciones provistas, se encuentra la banca móvil, la banca por Internet y la billetera digital.

Conforme a lo establecido en la Sección 9. de las normas sobre “Requisitos mínimos para la gestión y control de los riesgos de la tecnología y seguridad de la información” deberán considerar los aspectos de la seguridad de la información en todo el ciclo de vida de los dispositivos y aplicaciones provistos a los clientes.

Deberán aplicar controles tales como:

a. los datos intercambiados deben permanecer cifrados durante toda la interacción con el cliente,

b. implementar medidas para detectar y finalizar la sesión de cliente no autorizada,

c. inhabilitar el servicio e impedir el ingreso de factores de autenticación del cliente cuando se produzcan fallas que comprometan la seguridad del servicio, y

d. cuando se redirija al cliente del servicio financiero digital a sitios de terceros que permitan la ejecución de transacciones bancarias, los factores de autenticación del cliente no deben compartirse con esas terceras partes.

3.2.1 Aplicaciones provistas por la organización.

En la implementación de aplicaciones en entornos controlados por el cliente, el sujeto alcanzado debe establecer como mínimo los siguientes controles:

a. Utilizar métodos de instalación que limiten la exposición de datos personales, financieros o de los factores de autenticación del cliente.

b. Informar al cliente los criterios de admisibilidad de los dispositivos del cliente, así como las limitaciones de hardware, software, conectividad y entorno para su uso. Asimismo, deberán informar los requisitos de seguridad aplicables a los dispositivos propios del cliente.

c. Impedir el acceso a través de un dispositivo que no satisface los criterios de admisibilidad determinados.

d. Aplicar medidas que mitiguen los riesgos vinculados con las configuraciones del sistema operativo de los dispositivos móviles.

e. Solicitar exclusivamente los permisos mínimos necesarios para operar en la aplicación.

f. Como parte de los elementos de identificación, asociar la aplicación con el dispositivo móvil y con el cliente, tanto en el momento del alta o en una posterior reinstalación

g. Validar que el dispositivo en uso sea el asociado por el cliente e implementar controles de cambio de chip y de la línea utilizada.

h. Prever mecanismos de bloqueo de acceso a la aplicación y bloqueo automático de la sesión por inactividad (“time out”).

3.2.2. Dispositivos provistos por la organización.

Los dispositivos deberán estar identificados y autenticados para operar.

Los procesos de homologación de los dispositivos que permiten interactuar con el cliente deberán incluir una verificación y aprobación formal antes de su habilitación.

Cuando los dispositivos utilicen teclados físicos o virtuales, los factores de autenticación deberán ser cifrados inmediatamente después de su ingreso. Además, los datos de autenticación no deberán ser almacenados en el dispositivo provisto por la organización ni conservados en el registro de actividad.

3.2.2.1. Protección de los registros de auditoría.

Deberán implementar medidas de protección de los registros de auditoría, tanto digitales como impresos. Los controles aplicados deberán ser acordes a los resultados de los análisis de riesgos y evaluar como mínimo:

a. las condiciones de almacenamiento,

b. los mecanismos para su traslado,

c. las técnicas o métodos de borrado y/o destrucción segura de los soportes utilizados, y

d. las medidas de control de acceso.

3.2.2.2. Controles físicos en los dispositivos provistos.

Los dispositivos deben incorporar características que reduzcan el riesgo de copia, obstrucción, visualización de terceros o retención ilegal de factores de autenticación y valores monetarios, considerando, pero no limitándose a la aplicación de los siguientes controles:

a. Detectores de objetos adosados a dispositivos provistos por la organización.

b. Componentes anti-skimming en el ingreso de los factores de autenticación.

c. Mecanismos de detección de apertura, violación o alteración de las condiciones físicas y/o lógicas del dispositivo.

3.2.2.3. Controles en el mantenimiento, configuración, apertura, carga y balanceo de dispositivos provistos.

Los procesos de mantenimiento, configuración, apertura, carga y balanceo de dispositivos provistos por la organización deberán:

a. Implementar una segregación física y lógica entre las actividades de administración (instalación, configuración y ajuste de parámetros en el sistema operativo y aplicativo) y la operación del dispositivo (ejecución de tareas operativas de consulta, balanceo y reporte).

b. Aplicar en la apertura y cierre de dispositivo y tesoro un control dual para el uso y posesión temporal de las llaves físicas y/o lógicas.

c. Prever tareas de control desde la organización entre la documentación de respaldo y actividades operativas registradas.

3.2.2.4. Comprobante de la transacción.

Los dispositivos provistos por la organización deberán brindar al cliente la posibilidad de imprimir o enviar el comprobante de la transacción efectuada al punto de contacto previamente indicado.

3.3. Identificación digital de clientes.

Cuando los sujetos alcanzados admitan la identificación de personas humanas en forma digital y no presencial, deberán diseñar procesos que permitan corroborar la correspondencia unívoca de los datos o elementos requeridos con los datos de la persona humana que se pretende identificar.

Durante el proceso de identificación del cliente deberá aplicar controles para determinar cómo mínimo lo siguiente:

a. validación de la presencia real de la persona humana con prueba de vida,

b. validación de los puntos de contacto declarados y del dispositivo móvil asociado al cliente, y

c. validación de los elementos biométricos y la documentación presentada con organismos públicos.

Se deberán utilizar técnicas complementarias para verificar la identidad del cliente del servicio financiero en el proceso de alta digital de acuerdo con los resultados de los análisis de riesgos y la efectividad de los controles implementados.

3.3.1. Proceso de alta no concretada.

En caso de que el proceso de alta no se concrete, deberán aplicarse los siguientes controles sobre los datos recopilados durante el proceso:

a. No comunicar al cliente los motivos de los errores o fallas ocurridos en el proceso de identificación.

b. Los datos recolectados deberán ser eliminados mediante un proceso de borrado seguro.

c. Los datos conservados con fines estadísticos deberán ser desasociados o anonimizados.

3.4. Control de accesos. Requisitos para los factores de autenticación.

Los valores asociados a los identificadores de acceso utilizados en los servicios financieros digitales no podrán incluir datos personales o públicos del cliente y se deberá ofrecer opciones que permitan su modificación.

Deberán establecer las siguientes medidas mínimas para la protección de los factores de autenticación de los clientes de servicios financieros digitales durante todo su ciclo de vida:

a. no podrán ser conocidos por el personal de la organización o de terceras partes,

b. podrán ser almacenados únicamente para su verificación, implementando medidas adicionales para resguardar su confidencialidad, y

c. deberán implementar técnicas criptográficas para su protección.

Los factores de autenticación implementados deberán considerar las disposiciones establecidas en el punto 5.7.2. de las normas sobre “Requisitos mínimos para la gestión y control de los riesgos de la tecnología y seguridad de la información”. Además, deberán aplicarse las disposiciones particulares definidas a continuación.

3.4.1. Secreto memorizado:

Los autenticadores basados en secretos memorizados (o algo que “sabe”) deben cumplir los siguientes controles:

a. Longitud mínima, no inferior a 8 caracteres.

b. Conformación de caracteres que incluyan letras minúsculas y mayúsculas, números y caracteres especiales.

c. Cambio en el primer uso de secretos memorizados generados por la organización.

d. Limitación de la exposición de los secretos memorizados durante su ingreso.

e. Limitación de la velocidad de ingreso mediante el acceso automatizado bajo ciertos escenarios (por ejemplo: Captcha).

f. Limitación de los intentos fallidos de ingreso. Definir una política de reinicio de contador de intentos fallidos acorde al análisis de riesgo.

g. En la creación o modificación, se deberá brindar información detallada a los clientes sobre requerimientos mínimos para la fortaleza del secreto memorizado y los motivos de rechazo.

3.4.2. Autenticación fuera de banda.

Los autenticadores fuera de banda deberán cumplir los siguientes controles:

a. No estar visible cuando el dispositivo receptor esté bloqueado.

b. Cumplir con los requisitos definidos para claves de un solo uso (OTP).

c. El uso de un dispositivo registrado para la lectura de criptogramas gráficos mostrados en pantalla.

3.4.3. Claves de un solo uso (OTP).

Cuando se utilicen autenticadores basados en claves de un solo uso (OTP), deberán implementar los siguientes controles:

a. Medidas de detección de posesión y control del dispositivo donde se muestra el OTP.

b. La definición de un tiempo de vigencia del valor generado no mayor a 120 segundos.

c. La definición de una longitud mínima de 6 dígitos.

d. Definición de una longitud de semilla que asegure la generación de valores únicos.

e. Cifrado de canal o de información transmitida.

3.4.4. Tarjetas de pago (débito, crédito o prepago) y elementos físicos de autenticación.

Los procesos de distribución de tarjetas de pago o tokens físicos deberán considerar, como mínimo, los siguientes controles:

a. Que no se distribuyan por el mismo medio los factores de autenticación que estén asociados.

b. Que se asegure la trazabilidad de las acciones efectuadas.

c. Los elementos de autenticación estén deshabilitados durante su distribución.

3.4.4.1. Reemplazo de los factores de autenticación provistos

De acuerdo con los resultados de los análisis de riesgos, se deberán reemplazar los factores de autenticación provistos por los sujetos alcanzados, como mínimo, cuando se produzcan situaciones como:

a. Vencimiento.

b. Denuncia de robo, pérdida o deterioro.

c. Desconocimiento de transacciones efectuadas.

d. Detección de posibles ciberincidentes o puntos de compromisos que lo afecten.

e. Detección de fallas de fabricación o generación, pérdida durante la distribución y/o almacenamiento.

3.4.4.2. Factores de autenticación retenidos o no entregados al cliente.

Estos factores deberán ser destruidos o desvinculados del cliente y sus cuentas en un período no mayor a 30 días hábiles.

3.4.4.3. Factores de autenticación basados en tarjetas con circuito integrado (chip).

Para el uso seguro de estos factores deberán considerar como mínimo los siguientes controles:

a. Mecanismos de autenticación dinámica de la tarjeta.

b. Mecanismos que impidan su duplicación o alteración.

c. Cifrado de los datos almacenados en el circuito integrados.

d. Inclusión de hologramas, códigos de seguridad, identificación de la marca y organización emisora.

e. La operación con lectura de banda magnética en las tarjetas debe estar limitada y justificada en aquellas que cuenten con un sistema dual (banda magnética y chip).

f. La tarjeta sin contacto que no cuente con un factor de autenticación adicional debe fortalecer el monitoreo de uso y transaccional.

3.4.4.4. Factores de autenticación basados en tarjetas con banda magnética

Para el uso seguro de estos factores las organizaciones deberán considerar al menos, los siguientes controles:

a. Que el código de verificación de la tarjeta no esté almacenado en la banda magnética.

b. Que se refuerce el monitoreo del uso y el transaccional de la tarjeta que no cuente con un factor de autenticación adicional.

Adicionalmente, el secreto memorizado (PIN) asociado a las tarjetas de pago deberá:

c. Poseer una longitud al menos de 4 dígitos.

d. No estar conformado por el mismo número.

e. No ser consecutivos.

f. El PIN debe autenticarse en línea.

3.5. Capacitación y concientización.

En función de lo establecido en el punto 5.5. de las normas sobre “Requisitos mínimos para la gestión y control de los riesgos de la tecnología y seguridad de la información”, las organizaciones deberán elaborar planes de capacitación y concientización específicos para los servicios financieros digitales que incluyan al menos:

a. Información sobre los puntos de contacto dispuesto por la organización y pautas para verificar si son genuinos.

b. Información sobre vías de contacto utilizadas por la organización para notificar a sus clientes de situaciones que podrían comprometer su seguridad. En especial, los cuidados a tener en cuenta para identificar las cuentas oficiales de las redes sociales de la organización.

c. Información referida a los aspectos configurables o parametrizables que tiene el cliente en el servicio financiero digital.

d. Recomendaciones específicas sobre el uso seguro y la configuración de dispositivos propios del cliente del servicio financiero.

e. Información sobre técnicas de ingeniería social y respecto de las medidas de seguridad para protegerse contra esas técnicas.

f. Recomendaciones específicas sobre el uso seguro de dispositivos o aplicaciones provistas por la organización.

g. Información sobre el procedimiento que debería seguir el cliente ante un desconocimiento de una operación, como efectuar denuncias, como actuar ante sospechas de fraudes o en situación de fraude en curso, entre otros.

Los planes deberán ser actualizados en función de los cambios de los productos y servicios puestos a disposición de los clientes. Para la actualización, se deberán considerar también los resultados del monitoreo transaccional, las nuevas técnicas de ataques y de la gestión de ciberincidentes.

3.6. Vías de comunicación.

Los sujetos alcanzados deberán proveer vías de comunicación, disponibles las 24 horas, a sus clientes del servicio financiero para la recepción, atención de consultas y denuncias, notificación de ciberincidentes y/o situaciones sospechosas. La organización deberá entregar al cliente un comprobante para que pueda dar seguimiento a la comunicación efectuada.

Además, las organizaciones deberán implementar mecanismos de comunicación alternativa con sus clientes con el objeto de notificar alarmas o alertas surgidas del monitoreo transaccional implementado. Las vías de comunicación deben estar documentadas, utilizar puntos de contacto del cliente previamente validados e informar sobre eventos tales como:

a. Alta, baja, vinculación o rehabilitación de factores de autenticación.

b. Modificación de datos personales o parámetros para transaccionar.

c. Información transaccional.

d. Los sujetos alcanzados deberán poner a disposición de sus clientes en los servicios financieros digitales información sobre:

- Fecha y hora de último acceso al servicio utilizado.

- Factores de autenticación próximos a vencer.

- Los registros de las transacciones efectuadas, que deberán estar disponibles en formato digital durante al menos 90 días.

4.1. Detección y análisis de eventos.

Los sujetos alcanzados deberán establecer un proceso para el registro y el análisis de la información vinculada con eventos de seguridad de los sistemas, las redes y la infraestructura tecnológica que soporte a los servicios financieros digitales, acorde a lo establecido en el punto 5.8. de las normas sobre “Requisitos mínimos para la gestión y control de los riesgos de la tecnología y seguridad de la información”.

Adicionalmente, todos los sistemas y aplicaciones que den soporte a los servicios financieros digitales deberán generar registros de auditoría que permitan asegurar la trazabilidad de cada una de las acciones realizadas, conforme a lo establecido en el punto 9.1. de las normas sobre “Requisitos mínimos para la gestión y control de los riesgos de la tecnología y seguridad de la información”.

4.2. Monitoreo de la actividad y transacción del cliente.

Conforme a lo establecido en el punto 3.1., los sujetos alcanzados deberán definir una estrategia de monitoreo que permita detectar actividades inusuales o transacciones sospechosas de sus clientes en los servicios financieros digitales.

Las soluciones de monitoreo transaccional implementadas deberán considerar los resultados de los análisis de riesgos, los patrones de comportamiento y las circunstancias habituales del uso de los servicios y los factores de autenticación utilizados. Además, deberán aplicar, al menos, los siguientes criterios:

a. La clasificación de ordenantes y receptores en base a características de su cuenta para la determinación de umbrales, patrones y alertas dinámicas.

b. Frecuencia de transacciones por tipo, monto de transacciones y saldos habituales de cuentas.

c. Factores de autenticación comprometidos, patrones de fraude conocidos, indicios de programas maliciosos en los dispositivos empleados.

d. Patrones de comportamiento del cliente en la utilización del dispositivo o la aplicación provista por la organización.

e. La identificación de puntos comunes de compromiso que puedan afectar a las transacciones cursadas por los clientes.

Adicionalmente, el monitoreo transaccional sobre los factores de autenticación entregados por la organización debe facilitar la detección, registro y control de situaciones que establezcan un compromiso de datos sensibles.

En función de las alertas detectadas, deberán definir modelos de acción acordes a los resultados de los análisis de riesgos, los patrones de comportamiento y las circunstancias habituales del uso de la aplicación y los factores de autenticación. Los modelos podrán combinar medidas de tipo preventivo, reactivo y asumido. A saber:

- Preventivo: como la actividad de ejecutar acciones de comunicación con el cliente por otras vías antes de confirmar operaciones.

- Reactivo: como la actividad de realizar acciones para comunicarse con el cliente en forma posterior a la confirmación de operaciones sospechosas.

- Asumido: como la acción de devolver las sumas involucradas ante los reclamos del cliente por desconocimiento de transacciones efectuadas.

Los sujetos alcanzados deberán aplicar un proceso de mejora continua a sus soluciones de monitoreo transaccional, los modelos de acción y la gestión de incidentes, de acuerdo con la evolución de las técnicas fraudulentas emergentes, y la información sobre tendencias de fraude recopilada de fuentes internas o externas.

Deberán monitorear el uso y la evolución de técnicas de ingeniería social dirigidas a la organización, sus clientes y las terceras partes involucradas en los servicios.

Deberán tomar acciones preventivas y oportunas en la eliminación de cuentas y aplicaciones apócrifas, sitios falsos y contenido malicioso.

Los procesos de detección y monitoreo deberán estar integrados con la gestión de ciberincidentes, conforme a lo establecido en la Sección 8. de las normas sobre “Requisitos mínimos para la gestión y control de los riesgos de la tecnología y seguridad de la información” y las disposiciones del texto ordenado sobre “Lineamientos para la respuesta y recuperación ante ciberincidentes”.

Las siguientes definiciones se complementan con las normas sobre “Requisitos mínimos para la gestión y control de los riesgos de la tecnología y seguridad de la información” y con el glosario publicado en línea en la siguiente dirección URL:

https://www.bcra.gob.ar/SistemasFinancierosYdePagos/Ciberseguridad.asp#Glosario

Anti-skimming: se refiere a sistemas para combatir los delitos en cajeros automáticos o similares, prevenir el robo de identidad y reducir el fraude.

Aplicaciones apócrifas: hace referencia a las aplicaciones que aparentan ser legítimas. Por lo general, pueden estar disponibles en tiendas de aplicaciones o sitios web oficiales o no, para los distintos sistemas operativos móviles del mercado. Los ciberdelincuentes los diseñan y nombran de tal manera que parezcan verdaderas.

Cliente del servicio financiero: el término “cliente del servicio financiero” se refiere a la persona humana o jurídica que se encuentra identificada y suscrita a los servicios de una o más sujetos alcanzados.

Journal o tira de auditoría: comprende a los mecanismos físicos o lógicos dispuestos para el registro de la actividad de acceso a los servicios e instrucción de operaciones de los dispositivos provistos por la organización.

Modelos de acción de monitoreo transaccional: pautas y/o medidas a aplicar ante la detección de transacciones inusuales o sospechosas. Pueden combinar medidas de tipo:

- Preventivo: ejecutar acciones de comunicación con el cliente por otras vías antes de confirmar operaciones.
- Reactivo: lanzar acciones de comunicación con el cliente en forma posterior a la confirmación de operaciones sospechosas.
- Asumido: asumir la devolución de las sumas involucradas ante los reclamos del cliente por desconocimiento de transacciones efectuadas.

PSP: Proveedor de servicio de pagos, de acuerdo con las disposiciones establecidas en las normas sobre “Proveedores de servicios de pago”.

Servicio financiero digital: prestación de servicios financieros transaccionales, de consulta o de pago, proporcionados por las organizaciones a sus clientes en línea.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

B.C.R.A.	ORIGEN DE LAS DISPOSICIONES CONTENIDAS EN LAS NORMAS SOBRE "REQUISITOS MÍNIMOS PARA LA GESTIÓN DE LOS RIESGOS DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN ASOCIADOS A LOS SERVICIOS FINANCIEROS DIGITALES"

TEXTO ORDENADO			NORMA DE ORIGEN					OBSERVACIONES
Secc.	Punto	Párr.	Com.	Anexo	Sec.	Punto	Párrafo.	
1.	1.1.		"A" 7783			1.		
	1.2.		"A" 7783			1.		
2			"A" 7783					
3.	3.1.		"A" 7783			1.		
	3.1.		"A" 7783			1.		
	3.3.		"A" 7783			1.		
	3.4.		"A" 7783			1.		
	3.5.		"A" 7783			1.		
4.	4.1.		"A" 7783			1.		
	4.2.		"A" 7783			1.		
5.			"A" 7783			1.		

-Índice-

1.1. Sujetos obligados

1.1.1. Entidades financieras.
1.1.2. Infraestructuras del Mercado Financiero conocidas como Sistemas de Pago de importancia sistémica: INTERBANKING, COELSA, LINK y PRISMA.

1.2. Aspectos generales

Los sujetos obligados indicados en el punto 1.1., que a los efectos de esta norma denominaremos “entidades”, deberán asegurar la implementación de prácticas efectivas para el control interno y la gestión de riesgos de su entorno operativo de tecnología y seguridad de la información. Para ello, deberán demostrar comprensión de los riesgos y establecer un marco para su gestión acorde a la complejidad de los servicios financieros ofrecidos y de la tecnología que los soporta.

Las secciones siguientes establecen un conjunto de requisitos mínimos, aplicables a los procesos, estructuras y activos de información, que las entidades deberán implementar con el propósito de:

- Definir e implementar un marco de gestión de riesgos de la tecnología y la seguridad de la información como parte de la gestión integral de riesgos de la entidad.
- Definir marcos para el gobierno y la gestión de la tecnología y seguridad de la información, acordes con la gestión del riesgo.
- Alinearse con los objetivos de resiliencia operacional.
- Incluir procesos de mejora continua en los marcos de gestión.

Adicionalmente las entidades deberán promover:

- Una cultura de gestión de riesgos de tecnología y seguridad de la información que les permita identificar e implementar controles adicionales a estos requisitos mínimos.
- La adopción del “modelo de las tres líneas” en la definición de roles y responsabilidades.
- La adopción de marcos de referencia y estándares internacionales que permitan complementar los requisitos mínimos relacionados con riesgos, tecnología y seguridad de la información.

Activo: recurso de valor tangible o intangible que debería ser protegido, lo que comprende personas, información, infraestructura, finanzas y reputación.

Activo de información: datos, información, software (programas, aplicaciones, sistemas de información, bases de datos), hardware.

Amenaza: circunstancia que podría explotar una o más vulnerabilidades y afectar la ciberseguridad.

Anomalía: evento, comportamiento o funcionamiento no esperado.

Apetito de riesgo: estimación que indica cuánto riesgo la organización está dispuesta a aceptar dentro de sus operaciones habituales.

Aprendizaje automático (*machine learning*): rama de la inteligencia artificial que consiste en conseguir que un ordenador extraiga conclusiones a partir del análisis estadístico de los datos que se introducen, mediante un proceso que va mejorando de modo automático conforme se incorpora más evidencia al algoritmo.

Arquitectura empresarial: modelo que describe el conjunto completo de sistemas de información de una entidad: cómo están configurados, cómo están integrados, cómo interactúan con el entorno externo, cómo se operan para respaldar la misión y cómo contribuyen a los objetivos estratégicos.

Autenticación: proceso diseñado para establecer la fuente de la información, la validez de una transmisión, mensaje u emisor, o una forma para verificar la autorización de un individuo para recibir o acceder a categorías específicas de información.

Autenticación fuera de banda: uso de dispositivos físicos en posesión del usuario, que tienen una identificación unívoca y se comunican con la entidad por un canal distinto que la aplicación en la que el usuario opera. Su objetivo es probar la posesión y el control del dispositivo por parte del solicitante.

Autenticación multifactor (MFA): proceso de autenticación que requiere de más de un factor para que el solicitante obtenga acceso a los recursos o información. Para lograr la autenticación, deben ser correctos todos los factores presentados. La autenticación multifactor se puede implementar de tres (3) formas:

- **Autenticación adaptativa o basada en riesgo:** se asigna un valor de riesgo a la autenticación del usuario en función de su contexto y se define a partir de qué nivel de riesgo se piden factores de autenticación adicionales.
- **Autenticación basada en dispositivo autorizado:** cuando el solicitante inicia sesión desde un dispositivo que no ha sido previamente autorizado, se le solicitarán múltiples factores.
- **Autenticación MFA permanente por solicitante:** el recurso al que se quiere acceder requiere el uso de MFA cada vez que un solicitante requiere acceso.

El método de MFA de dos factores (2FA) consiste en la utilización de una combinación de dos (2) factores de distintas categorías.

Ciberincidente o Incidente de tecnología y seguridad: evento cibernético que:

- pone en peligro la ciberseguridad de un sistema de información o la información que el sistema procesa, almacena o transmite; o
- infringe las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable, sea o no producto de una actividad maliciosa.

Ciberresiliencia / resiliencia tecnológica: capacidad de una organización de continuar llevando a cabo su misión anticipando y adaptándose a las amenazas y otros cambios relevantes en el entorno, y resistiendo, conteniendo y recuperándose rápidamente de ciberincidentes.

Ciberseguridad: preservación de la confidencialidad, integridad y disponibilidad de información y / o sistemas de información a través de un medio cibernético. Además, otras propiedades, como la autenticidad, la rendición de cuentas, el no repudio y la confiabilidad también pueden ser involucradas.

Códigos de un solo uso (OTP): clave, contraseña o códigos de un solo uso generados por software o mediante un dispositivo.

Código malicioso *(malware*): software con un objetivo malicioso y que contiene características o capacidades que podrían provocar un daño directo o indirecto a entidades o a sus sistemas de información.

Componentes de gobierno: los procesos, la estructura organizativa; las personas, habilidades y competencias; las políticas, normas y procedimientos, y la cultura y liderazgo que forman parte de un marco de gobierno.

Confiabilidad: uniformidad en cuanto al comportamiento y los resultados deseados.

Confidencialidad: propiedad de la información de no ser puesta a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Continuidad del negocio: capacidad de una organización para continuar brindando productos y servicios dentro de plazos aceptables, y con una capacidad predefinida, durante una disrupción.

Dato: Pieza de información.

Datos del cliente: la información del cliente que permita revelar o inferir su identidad, credenciales personales, relación comercial y/o posición financiera, limitada, restringida y/o protegida por la Ley de Datos Personales (Ley 25.326), la Ley de Entidades Financieras (Ley 21.526) y normas particulares del BCRA.

Datos contables: información referida a saldos, balances y activos de la entidad financiera o de sus clientes no individualizados.

Datos transaccionales: instrucciones individuales o relacionadas que ordenen movimientos financieros en cuentas de uno o varios clientes, pasibles de verificación y aprobación antes de su perfeccionamiento o confirmación.

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Dispositivos criptográficos: son dispositivos que contienen una o varias claves secretas (simétricas o asimétricas) que utilizan para realizar una operación criptográfica para la autenticación (normalmente una firma). Los dispositivos criptográficos también pueden ser de uno o varios factores:

- **Dispositivos criptográficos de un factor:** realiza la operación criptográfica cuando el verificador se lo solicita.
- **Dispositivos criptográficos multifactor:** requiere la activación mediante un segundo factor de autenticación del tipo “algo que se sabe” o biométrico, para realizar la operación criptográfica.

Dispositivos de generación de códigos de un solo uso: dispositivo que generan códigos de un solo uso. Un dispositivo se considera multifactor cuando requiere de algún factor de autenticación previo para acceder al código de un solo uso.

Disrupción: evento que causa una desviación negativa no planificada en la entrega de productos o servicios de acuerdo con los objetivos de la organización.

Evento: ocurrencia o cambio de un conjunto particular de circunstancias.

Evento de seguridad de la información: cualquier ocurrencia observable que sea relevante para la seguridad de la información. Esto puede incluir intentos de ataques o fallos que descubren vulnerabilidades de seguridad existentes. Los eventos de seguridad a veces indican que se está produciendo un ciberincidente.

Explicabilidad: capacidad de proporcionar información significativa, adecuada al contexto y coherente que permita comprender los resultados de la aplicación de técnicas de aprendizaje automático e inteligencia artificial.

Factores de Autenticación (FA): es una evidencia que sirve para demostrar al solicitante su identidad y, por lo tanto, superar la autenticación. Los factores de autenticación se dividen en tres (3) categorías:

- ***Algo que se sabe:*** la evidencia es algo que solo el solicitante puede saber. Por ejemplo, una contraseña o PIN.
- ***Algo que se tiene:*** la evidencia es algo que solo el solicitante puede poseer.
- ***Algo que se es:*** la evidencia es algo que solo el solicitante puede ser. En general, se trata de alguna característica biométrica.

Gestión de datos: desarrollo de actividades para establecer políticas, procedimientos y mejores prácticas que permitan asegurar que los datos sean comprensibles, confiables, visibles, accesibles e interoperables.

Gestión del ¡Error! Referencia de hipervínculo no válida. gestión coordinada del conjunto de los proyectos para lograr objetivos específicos de negocio.

Identificación: proceso por el cual alguien o algo que no se conoce de antemano se hace conocido.

Infraestructura tecnológica / infraestructura de TI: subconjunto de la infraestructura que comprende al hardware, redes, software y firmware.

Integridad: cualidad de exacto y completo.

Inteligencia artificial (IA): conjunto de teorías y de algoritmos que permiten llevar a cabo tareas que, típicamente, requieren capacidades propias de la inteligencia humana.

Inteligencia sobre amenazas (*threat intelligence)*: información sobre amenazas que ha sido agregada, transformada, analizada, interpretada o enriquecida para ofrecer el contexto necesario para los procesos de toma de decisiones.

Marco de gestión: refiere a un conjunto coordinado de procesos de planificación, implementación, operación, monitoreo y mejora continua.

Modelo de las 3 líneas: esquema que define 3 niveles para la asignación de roles y responsabilidades para una efectiva gestión de riesgos y control por oposición.

Plan de continuidad del negocio: recopilación documentada de procedimientos e información para su uso en un incidente con el objetivo de permitir que una organización continúe entregando sus productos y servicios críticos a un nivel aceptable.

Política: un documento que registra principios de alto nivel o un curso de acción acordado; dirección e intención generales expresadas formalmente.

Práctica: actividad realizada de manera recurrente.

Procedimiento: método compuesto por una secuencia de pasos que deben seguirse para completar la tarea o un proceso.

Propietario de la información: dentro de la organización, responsable formal de definir y velar por la integridad, confidencialidad y disponibilidad de una cierta información.

RPO (Recovery Point Objective): pérdida máxima de información tolerable en caso de interrupción.

RTO (Recovery Time Objective): Tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

Secreto memorizado (clave o contraseña): dato que se utiliza para autenticación. Puede ser creado por un usuario, o creado por la entidad y entregado al uso.

Seguridad de la información: la preservación de la integridad, disponibilidad y confidencialidad de la información. Además, podría incluir la autenticidad, la trazabilidad, la rendición de cuentas, el no repudio y la confiabilidad.
Shadow IT: se refiere a software, hardware, servicios y dispositivos no autorizados por la organización que operan en el entorno de TI.
Subcontratación: práctica en virtud de la cual una tercera parte encarga a un subcontratista parte de lo que se le ha encomendado.
Tercera parte: quien brinda procesos, servicios y/o actividades que han sido formalmente delegados por la entidad de acuerdo con lo establecido en la Sección 2. de las normas sobre “Expansión de entidades financieras”. Se considera dentro de esta definición a una entidad perteneciente a un grupo corporativo (global o doméstico) o una entidad externa al grupo corporativo, con la cual se ha establecido un contrato para la realización de procesos, servicios y/o actividades.
Tolerancia al riesgo: nivel aceptable de variación respecto del apetito de riesgo definido en el logro de los objetivos de la entidad.
Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

B.C.R.A.	ORIGEN DE LAS DISPOSICIONES CONTENIDAS EN LAS NORMAS SOBRE "REQUISITOS MÍNIMOS PARA LA GESTIÓN Y CONTROL DE LOS RIESGOS DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN"

TEXTO ORDENADO			NORMA DE ORIGEN				OBSERVACIONES
Sección	Punto	Párrafo	Com.	Cap.	Punto	Párrafo	
1.	1.1.		"A" 7724		2.		Según Com. "A" 7783.
	1.2.		"A" 7724		2.		
2.	2.1.		"A" 7724		2.		
	2.2.		"A" 7724		2.		
	2.3.		"A" 7724		2.		
3.			"A" 7724		2.		
4.	4.1.		"A" 7724		2.		
	4.2.		"A" 7724		2.		
	4.3.		"A" 7724		2.		
	4.4		"A" 7724		2.		
	4.5.		"A" 7724		2.		
	4.6.		"A" 7724		2.		
	4.7.		"A" 7724		2.		
5.	5.1.		"A" 7724		2.		
	5.2.		"A" 7724		2.		
	5.3.		"A" 7724		2.		
	5.4.		"A" 7724		2.		
	5.5.		"A" 7724		2.		
	5.6.		"A" 7724		2.		
	5.7.		"A" 7724		2.		
	5.8.		"A" 7724		2.		
6.	6.1.		"A" 7724		2.		
	6.2.		"A" 7724		2.		
	6.3.		"A" 7724		2.		
	6.4.		"A" 7724		2.		
	6.5.		"A" 7724		2.		
	6.6.		"A" 7724		2.		
	6.7.		"A" 7724		2.		
	6.8.		"A" 7724		2.		
7.	7.1.		"A" 7724		2.		
	7.2.		"A" 7724		2.		
	7.3.		"A" 7724		2.		
	7.4.		"A" 7724		2.		
	7.5.		"A" 7724		2.		
	7.6.		"A" 7724		2.		
	7.7.		"A" 7724		2.		
8.	8.1.		"A" 7724		2.		
	8.2.		"A" 7724		2.		
	8.3.		"A" 7724		2.		
9.	9.1.		"A" 7724		2.		
	9.2.		"A" 7724		2.		
10.	10.1.		"A" 7724		2.		
	10.2.		"A" 7724		2.		
	10.3.		"A" 7724		2.		
	10.4.		"A" 7724		2.		

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

"REQUISITOS MÍNIMOS PARA LA GESTIÓN Y CONTROL DE LOS RIESGOS DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN"							
TEXTO ORDENADO			NORMA DE ORIGEN				OBSERVACIONES
Sección	Punto	Párrafo	Com.	Cap.	Punto	Párrafo	
11.			"A" 7724		2.		