BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" **6017**	**15/07/2016**

A LAS ENTIDADES FINANCIERAS:

Ref.: Circular
RUNOR 1 - 1208

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

.

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

"1. Sustituir en las normas 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" los siguientes puntos:

"Índice

"6.1. Alcance.

Se encuentran alcanzadas las entidades financieras que intervengan en la prestación, por sí o por terceros en su nombre, de servicios financieros por intermedio de algunos de los siguientes Canales Electrónicos (CE), cuya definición y características se encuentra en el Glosario del punto 6.6.:

6.1.1. Cajeros Automáticos (ATM).

6.1.2. Terminales de Autoservicio (TAS).

6.1.3. Banca Móvil (BM).

6.1.4. Banca Telefónica (BT).

6.1.5. Banca por Internet (BI).

6.1.6. Puntos de Venta (POS).

6.1.7. Plataforma de Pagos Móviles (PPM).”

2. Sustituir en las normas 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” los siguientes puntos:

“6.2. Procesos de referencia.

De modo referencial y con el objetivo de facilitar la implementación de los requisitos de seguridad determinados en esta sección, la Gestión de Seguridad de los Canales Electrónicos se entiende como el ciclo de procesos que reúnen distintas tareas, especialidades y funciones, de manera integrada e interrelacionada, repetible y constante para la administración, planificación, control y mejora continua de la seguridad informática en los Canales Electrónicos.

Los Procesos de Referencia aquí señalados, reúnen el conjunto de tareas y especialidades que las entidades pueden poseer, con estas u otras denominaciones y en la composición orgánica que mejor atienda sus intereses y satisfaga las funcionalidades y propósitos descriptos. Asimismo, deben informar a la Gerencia de Auditoría Externa de Sistemas la estructura e interrelaciones orgánicas y operativas que en sus organizaciones se corresponda:”

“6.3.1.4. Los errores de encuadramiento detectados por las auditorías internas y/o externas obligan a las entidades a efectuar los ajustes correspondientes en un plazo no mayor a 180 días corridos posteriores a su notificación, debiendo presentar a la Superintendencia de Entidades Financieras y Cambiarias, un informe de las adecuaciones efectuadas avalado por una verificación de conformidad de su Auditoría Interna, posterior al vencimiento de plazo indicado. La Superintendencia de Entidades Financieras y Cambiarias podrá realizar una verificación de lo actuado.”

“6.3.3.5. Las propuestas de implementación de un nuevo CE o modalidad diferente de las contempladas en esta sección, previo un análisis de riesgo de la entidad financiera, deben ser informadas al menos con 60 días de anticipación a la Gerencia Principal de Seguridad de la Información, para que en conjunto con la Gerencia Principal de Sistemas de Pago y Cuentas Corrientes analicen los alcances particulares, características técnicas e impacto de la implementación y de corresponder brinden las eventuales recomendaciones que consideren necesarias o realicen los ajustes normativos que correspondiesen.”

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

"6.3.3.6. En todos aquellos casos en que la operación no esté asociada a una clave de identificación personal, ante el desconocimiento por parte del cliente de una transacción efectuada mediante POS o PPM, las entidades financieras deben proceder a la inmediata devolución/acreditación de los fondos al cliente, sin perjuicio de iniciar la investigación de la operación y eventualmente, las acciones administrativas y/o legales que correspondieran."

"6.4.2. Criticidad y Cumplimiento.

La criticidad es un ponderador que establece el nivel de importancia relativo de un escenario y sus necesidades regulatorias. Las entidades deben instrumentar los mecanismos necesarios para considerar la aplicabilidad del escenario a su contexto particular y su inclusión en la matriz de riesgo operacional de tecnología que emplee en su gestión de riesgo operacional acorde con lo indicado en los puntos 6.4.1. y subsecuentes.

El nivel de obligación de las entidades de cumplir los requisitos técnico-operativos está determinado por tres elementos: la criticidad asignada, la vigencia determinada en cada requisito técnico-operativo y los resultados de la gestión de riesgo de las entidades financieras.

Los valores de criticidad, los criterios utilizados para su asignación a cada escenario y el cumplimiento se determinan según lo indicado en la siguiente tabla.

Valor	Descripción	Criterios de asignación	Cumplimiento
1	Alta exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma extendida la disponibilidad de los servicios y la confiabilidad de el/los CE, la entidad financiera y el sistema financiero en general.	• Exposición al riesgo sistémico y propagación del efecto negativo. • Impacto económico sobre los clientes y la entidad financiera. • Nivel de penetración del Canal Electrónico y Medio de Pago asociado. • Interoperabilidad y efectos sobre otros CE.	Obligatorio. Las entidades financieras deben satisfacer los requisitos técnico operativos de cada escenario de acuerdo con la Tabla de Requisitos correspondiente (punto 6.7).
2	Moderada exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma limitada la disponibilidad y la confiabilidad de el/los CE involucrados, la entidad financiera y el sistema financiero en general.		Alineado. Las entidades deben realizar sus mejores esfuerzos para satisfacer los requisitos técnico-operativos de cada escenario, implementando medidas compensatorias y/o alternativas en aquellos requisitos que no satisfagan los indicados en la Tabla de Requisitos correspondiente (punto 6.7).
3	Baja exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma limitada la disponibilidad y la confiabilidad en el/los CE involucrados, la entidad financiera o el sistema financiero en general.		Esperado. Las entidades podrán satisfacer los requisitos de acuerdo con los resultados formales de su gestión de riesgo

La asignación de los valores en cada escenario, es una potestad de este Banco Central. No obstante, cuando no se encuentre asignado un valor a un determinado escenario, las entidades financieras deben asignarlo siguiendo los criterios establecidos en la tabla y los resultados formales de su gestión de riesgo operacional. Este Banco Central queda facultado para realizar actualizaciones periódicas de estos valores, adecuando los mismos de acuerdo con el resultado de sus verificaciones, el comportamiento del sistema financiero y el contexto nacional."

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

"6.5. Matriz de Escenarios.

Matriz de Escenarios					
Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
Credenciales y Medios de Pago	ECM001	Generación, distribución y descarte de credenciales que incluyen TC/TD.	ATM; TAS y POS.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC010; RCC013; RCC014; RCA001; RCA003; RCA009; RCA011; RCA012; RCA015; RCA016; RCA017; RCA018; RCA019; RCA020; RCA021; RCA031; RCA037; RCA038; RCA043; RCA044; RCA045; RIR002; RIR003; RIR005; RIR009; RGI001; RGI002; RGI003 y RGI005.
	ECM002	Generación, distribución y descarte de Credenciales que no incluyen TC/TD.	BI; BM; PPM y BT.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC010; RCC013; RCC014; RCA001; RCA003; RCA009; RCA011; RCA012; RCA014; RCA016; RCA017; RCA018; RCA019; RCA028; RCA029; RCA037; RCA043; RIR002; RIR003; RIR005; RIR009; RGI001, RGI002; RGI003 y RGI005.
	ECM003	Suscripción, presentación, uso, renovación y baja de credenciales que incluyen TD/TC.	ATM; TAS; PPM y POS.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC013; RCC014; RCA002; RCA003; RCA004; RCA005; RCA006; RCA007; RCA008; RCA009; RCA010; RCA011; RCA012; RCA013; RCA015; RCA017; RCA018; RCA022; RCA023; RCA025; RCA026; RCA030; RCA031; RCA036; RCA040; RCA041; RCA044; RCA045; RCA048; RIR001; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR015; RIR016; RMC005; RMC006; RMC007; RMC008; RMC009; RMC010; RGI001, RGI002; RGI003 y RGI005.
	ECM004	Suscripción, presentación, uso, renovación y baja de credenciales sin TD/TC.	BI; BM; PPM; TAS y BT.	**1**	RCC001; RCC002; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCC014; RCA002; RCA003; RCA004; RCA005; RCA007; RCA008; RCA009; RCA010; RCA011; RCA012; RCA014; RCA017; RCA018; RCA022; RCA023, RCA024; RCA026; RCA027; RCA028; RCA030; RCA039; RCA040; RCA041; RCA042; RIR001; RIR002; RIR003; RIR004; RIR005; RIR007; RIR009; RIR015; RIR016; RMC001; RMC005; RMC006; RMC008; RMC010; RGI001, RGI002; RGI003 y RGI005.

Matriz de Escenarios (continuación)					
Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
Dispositivos/Aplicaciones	EDA001	Diseño, funcionalidad y homologación de dispositivos suministrados por la entidad o el operador.	ATM; POS y TAS.		RCC006; RCC012; RCC010; RCC013; RCA020; RCA033; RCA034; RCA036; RCA037; RCA038; RIR001; RIR002; RIR003; RIR004; RIR005; RIR009; RIR010 y RIR011.
	EDA002	Compatabilización de dispositivos propios del usuario.	BI; BT; PPM y BM.	**2**	RCC006; RCC010; RCC011; RCC013; RCA034; RCA035; RCA037; RIR012; RIR017 y RIR019.
	EDA003	Diseño, funcionalidad y homologación de aplicaciones para la interacción del usuario con el CE, suministrados por la entidad/operador.	BI; BT; PPM y BM.		RCC006; RCC010; RCC012; RCC013; RCA027; RCA033; RCA034; RCA037; RIR001; RIR002; RIR003; RIR004; RIR005; RIR009; RIR010; RIR011; RIR012 y RIR017.
	EDA004	Operaciones y mantenimiento de dispositivos/aplicaciones con manejo físico de valores.	ATM; TAS y POS.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC009; RCC010; RCC012; RCC013; RCA012; RCA013; RCA015; RCA018; RCA023; RCA026; RCA033; RCA037; RCA040; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR010; RIR014; RIR015; RIR018; RMC003; RMC006; RMC007; RMC009; RMC010; RMC012; RMC013; RGI001; RGI002; RGI003 y RGI005.
	EDA005	Operaciones y mantenimiento de dispositivos/aplicaciones sin manejo físico de valores.	BI; BT; PPM y BM.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC009; RCC010; RCC012; RCC013; RCA012; RCA013; RCA014; RCA018; RCA023; RCA026; RCA033; RCA037; RCA040; RIR002; RIR003; RIR004; RIR005; RIR007; RIR009; RIR010; RIR014; RIR015; RMC001; RMC003; RMC006; RGI001; RGI002; RGI003 y RGI005.

Matriz de Escenarios (continuación)					
Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
Transacciones	ETR001	Depósito de valores físicos en el CE con destino directo a cuentas bancarias o pagos de bienes y servicios.	ATM y TAS.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC013; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC006; RMC008; RMC009; RGI001; RGI002; RGI003 y RGI005.
	ETR002	Extracción de efectivo por CE.	ATM.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC013; RCA032; RCA040; RCA046; RCA047 RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Matriz de Escenarios (continuación)					
Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
	ETR003	Pago de bienes o servicios.	ATM; TAS; POS; BI; BM; PPM y BT.	**2**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR004	Transferencias de fondos entre cuentas de un mismo titular y misma entidad financiera.	ATM; TAS; BI; BM y BT.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR005	Transferencias Inmediatas.	ATM ; BM y BI.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR006	Transferencias ordinarias	ATM; TAS; BI y BM.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR007	Solicitud, formalización y acreditación de operaciones de crédito.	ATM; TAS; BI y BM.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR008	Transacciones de consulta, instrucción operativa o instrucción financiera con confirmación por vía tradicional.	ATM; TAS; BI; BT y BM.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC006; RMC008; RMC009; RGI001; RGI002; RGI003 y RGI005.
	ETR009	Nuevas operatorias transaccionales no contempladas en otros escenarios, con o sin movimiento de fondos.	ATM; TAS; POS; BI; BT; PPM y BM.	**2**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032, RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR010	Transacciones de Bajo Valor: extracciones de efectivo, pago de bienes y/o servicios y transferencias inmediatas.	ATM; POS; BI; BM y PPM	**2**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003; RGI005"

"6.6. Glosario de términos utilizados en la Sección 6.

Se incluye, en orden alfabético, la definición aplicable a los términos y acrónimos utilizados en esta sección con objeto de facilitar la interpretación y ofrecer mayor claridad a los contenidos.

Activo. Comprende a los recursos, personas y medios indispensables para la ejecución de uno o más procesos de negocios que sean relevantes en los resultados esperados de estos últimos.

Autenticación Fuerte - Doble Factor. Comprende la utilización combinada de dos factores de autenticación, es decir dos elementos de las credenciales de distinto factor. Complementariamente, considérese lo expuesto sobre **Factores de Autenticación** y **Credenciales**.

Banca Electrónica. Comprende a todo servicio bancario y/o financiero, ofrecido por una entidad y basado en el uso de tecnología para la ejecución de operaciones y transacciones por parte de un usuario de servicios financieros, con mínima o ninguna asistencia o

participación de un operador humano. La Banca Electrónica incluye pero no se limita a la implementación de Canales Electrónicos con las características indicadas en esta norma.

Banca Móvil (BM). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros, que se basan en la utilización de aplicaciones (programas) informáticas diseñadas para su implementación y operación en dispositivos móviles propios 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) y se comunican, 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.

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 propios del usuario, 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 datos bajo administración de un operador público o privado.

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.

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.

Cliente - usuario de servicios financieros - usuario. Los términos "cliente" y "usuario de servicios financieros" son equivalentes y se refieren a la persona física o jurídica que se encuentra identificada y suscrita a los servicios de una o más entidades financieras. El término "usuario" es una denominación genérica aplicable a clientes y no clientes.

Contramedidas. Comprende a todas las acciones, planes, tareas operativas, mecanismos de software o hardware dispuestos para mitigar el riesgo de ocurrencia de ataque o compromiso de una vulnerabilidad conocida.

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 dispositivo (factor basado en "algo que tiene").

Control dual. Comprende al proceso que 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. Complementariamente, considérese lo expuesto sobre **Factores de Autenticación**.

Datos personales públicos. Comprende a 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, así como otros usuarios calificados para el mantenimiento y control en sitio. Incluye los elementos lógicos y/o aplicaciones necesarios para brindar funcionalidad y operación a los elementos físicos.

Encripción - métodos. Comprende a los métodos para el cifrado de información con el propósito lograr confidencialidad de su contenido y limitar su revelación a la aplicación de un mecanismo de descifrado previsto. Algunos métodos considerados en esta norma, incluyen, pero no se limitan a DES ("Data Encryption Standard"), 3DES (triple cifrado del DES), entre otros.

Escalamiento - Escalamiento de incidentes. Comprende al protocolo formal y procedimientos específicos para el flujo de ejecución e informe de las actividades de recepción, diagnóstico, análisis, contención, corrección y reporte de los incidentes de seguridad en los Canales Electrónicos.

Evento de seguridad. Comprende al hecho ocurrido e identificado sobre el estado de un sistema, servicio o red que indique un desvío de la política de seguridad establecida, una falla de las medidas de seguridad implementadas o una situación desconocida previamente que pueda ser relevante a la seguridad.

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).

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.

Incidente de seguridad en Canales Electrónicos. Se conforma por el evento o serie de eventos de seguridad, operativos y tecnológicos interrelacionados que generen una exposición no deseada o esperada de las credenciales, transacciones, datos de los clientes y el servicio bancario asociado y que posean una probabilidad significativa de comprometer las operaciones y amenazar la seguridad informática.

Infraestructura de redes. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento y transporte de voz y datos que interconectan e integran los recursos de la infraestructura de tecnología y sistemas.

Infraestructura de seguridad. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento y control de la plataforma tecnológica asociada a la seguridad de los Canales Electrónicos.

Infraestructura de tecnología y sistemas. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento, procesamiento y control de los servicios de tecnología informática asociada a los Canales Electrónicos.

Journal o Tira de auditoría. Comprende a los mecanismos físicos y/o lógicos dispuestos para el 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.

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.

Operadores. Se utiliza el término en forma indistinta para indicar a las empresas prestadoras de servicios financieros dentro de los indicados en esta sección, que cuenten con un acuerdo de servicio con las entidades financieras o actúen en su nombre o cuyas operaciones afecten las cuentas de crédito y/o depósito de sus clientes.

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 con acuerdo de las entidades financieras y operadores de transacciones financieras del Sistema Financiero Nacional

Punto de compromiso. Comprende al individuo, empresa o comercio adquirente de POS en el que se detecta un patrón similar de operaciones sospechosas o fraudulentas con TD/TC.

Puntos de venta (POS). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio al consumidor financiero, que se basan en la utilización de distintos medios de pago electrónico (Tarjetas de Débito/Crédito) para el pago de servicios u operaciones financieras que generen un débito o un crédito en las cuentas bancarias que el cliente posee con el emisor y que confirman tales operaciones mediante la comunicación local o remota con un centro de procesamiento de la entidad emisora o tercero interesado con acuerdo previo del emisor, mediante redes públicas de comunicación aptas y aprobadas por autoridad competente para la transmisión de datos bajo administración de un operador público o privado.

Redes privadas y públicas. Infraestructura de comunicaciones se considera privada cuando es administrada por una entidad financiera o un tercero en su nombre y accesible de forma exclusiva y única para la infraestructura de tecnología y sistemas de la entidad financiera. Se considera pública cuando la infraestructura de comunicaciones es administrada por un operador independiente y accesible mediante suscripción previa a múltiples empresas o individuos.

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

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. Se entenderá compuestos 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 por la persona/comercio y la composición del mensaje correspondiente), ***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.

Tarjetas de Débito/Crédito (TD/TC). Comprende a elementos asociados a las credenciales de acceso a algunos Canales Electrónicos, habitualmente basados en piezas plásticas cuyas inscripciones y características físicas las hacen aptas para su presentación y lectura en dispositivos de autenticación y autorización de los mismos. En la presente norma se mencionan en dos modalidades habituales de uso, como medios primarios de

transacciones comerciales de crédito/débito o como medios primarios de acceso a operaciones financieras por ATM ("Automated Teller Machine").

Telefonía fija. Servicios de comunicación ofrecidos por empresas de telecomunicaciones que utilizan los espectros de telefonía fija o terrestre autorizados a nivel nacional, y que incluyen los servicios de enlace e intercambio de voz y datos. Requiere una suscripción personal o comercial con locación del servicio en domicilio específico.

Telefonía móvil. Servicios de comunicación ofrecidos por empresas de telecomunicaciones que utilizan los espectros de telefonía móvil autorizados a nivel nacional, y que incluyen los servicios de enlace e intercambio de voz y datos. Requiere suscripción personal o comercial pero es independiente de la locación del suscriptor.

Terminales de autoservicio (TAS). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio al cliente bancario, que se basan en la utilización de los dispositivos conocidos como Terminales de Autoservicio u otros de similar naturaleza, enlazados a la red institucional de la entidad responsable, ya sea por conexión directa o indirecta (sucursal, proveedor) a un centro de procesamiento y que permitan por lo menos el depósito y transferencia de fondos y excluyan la extracción de efectivo sin intervención de un operador humano.

Transacciones de Bajo Valor. Transacciones financieras por medio de Canales Electrónicos habilitados hasta el máximo establecido en la Comunicación "A" 5982 y sus modificatorias."

"6.7. Tablas de requisitos técnico-operativos.

6.7.1. Tabla de requisitos de Concientización y Capacitación.

Tabla de requisitos de Concientización y Capacitación		
Código de requisito	**Descripción de requisito**	**Alcance**
RCC001	Los contenidos del programa de CC deben formularse y mantenerse actualizados en base a un análisis de las vulnerabilidades y los resultados de la Gestión de Incidentes, e incluir, pero no limitarse a incidentes: reportados, detectados y conocidos.	
RCC002	Los contenidos del programa de CC deben incluir: técnicas de detección y prevención de apropiación de datos personales y de las credenciales mediante ataques de tipo "ingeniería social", "phishing", "vishing" y otros de similares características.	
RCC003	Los contenidos del programa de CC deben incluir: técnicas de detección y prevención del "skimming" y apropiación de datos de las credenciales mediante técnicas de intervención física.	
RCC004	Los contenidos del programa de CC deben incluir: técnicas de detección de situaciones sospechosas en el recinto o entorno de acceso al CE.	
RCC005	Mantener informado al personal interno, personal responsable por la gestión del CE, personal de terceros involucrado en las tareas operativas y clientes sobre las vías de comunicación para la recepción de denuncias o problemas en el circuito asociado al escenario descripto.	
RCC006	Respecto de la audiencia del programa de CC, deben aplicarse los siguientes criterios: a. Características y segmentación de la audiencia, de acuerdo con el nivel de intervención en el proceso y naturaleza de la función o rol que ocupa cada participante. b. Deben encontrarse alcanzados todos los participantes necesarios en el flujo completo de la actividad indicada en el escenario. c. Orientado pero no limitado a: personal interno, personal responsable por la gestión del CE, proveedores y clientes.	
RCC007	Con una periodicidad mínima anual, debe efectuarse un análisis del Programa de CC ejecutado que mida la evolución de los incidentes, respecto de las actividades de CC realizadas incluyendo como mínimo: a. Un reporte de la cantidad y segmentación de destinatarios y contenidos del	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de requisitos de Concientización y Capacitación		
Código de requisito	**Descripción de requisito**	**Alcance**
	programa de CC. b. Una comparación entre los contenidos cubiertos por el programa de CC y la cantidad y tipo de incidentes de seguridad reportados/detectados/conocidos.	
RCC008	Los contenidos del programa de CC deben incluir: medidas y técnicas para la protección de la privacidad de las credenciales.	
RCC009	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre el uso seguro de los dispositivos propios del usuario y los dispositivos provistos por la entidad/operador.	
RCC010	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre las prácticas de seguridad en la plataforma de soporte de CE.	
RCC011	Los contenidos del programa de CC deben incluir: acciones específicas del usuario para la configuración de los dispositivos propios para comunicación con el CE (teléfonos, computadores personales, tabletas electrónicas, entre otros). Incluye pero no se limita a las características diferenciadas por dispositivo para el almacenamiento de datos, reposo/bloqueo automático, eliminación de información antes del descarte o reemplazo del dispositivo, actualización de sistemas operativos y piezas de software provistas por la entidad para uso del CE.	
RCC012	Los contenidos del programa de CC deben incluir técnicas específicas para el desarrollo/adquisición/fabricación, implementación, homologación y prueba de características de seguridad de los dispositivos y piezas de software provisto por la entidad/operador, asegurando que el personal involucrado interno/externo se encuentra debidamente capacitado para disminuir las fallas de implementación de las características de seguridad.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

6.7.2. Tabla de requisitos de Control de Acceso.

Tabla de requisitos de Control de Acceso		
Código de requisito	**Descripción de requisito**	**Alcance**
RCA001	Los procesos de distribución de elementos de identificación y autenticación basados en el factor "algo que sabe" deben ser siempre separados de la distribución de los elementos basados en el factor "algo que tiene".	
RCA002	La renovación de factores de identificación y autenticación basados en "algo que sabe" debe permitir la autogestión del cliente bancario o la mínima intervención de un operador durante el proceso, asegurando que solamente el cliente conocerá los valores asignados.	
RCA003	Los elementos de autenticación basados en el factor "algo que sabe" no deben ser conocidos antes ni durante su generación y uso por los funcionarios, empleados, representantes o terceros vinculados con las actividades correspondientes al escenario.	
RCA004	El almacenamiento de valores correspondientes a los factores de autenticación de los clientes bancarios, sólo será permitido cuando estos se encuentren protegidos mediante técnicas que impidan su conocimiento a otros diferentes del cliente y sólo con propósitos de verificación automática de las credenciales presentadas por el cliente para acceder y/o confirmar operaciones en el CE.	
RCA005	Las habilitaciones y rehabilitaciones de los elementos de identificación y autenticación basados en el factor "algo que tiene" deben ser efectuadas mediante un proceso que garantice la identificación positiva del titular (RCA040). Asimismo, estos elementos, sólo podrán estar vinculados durante su uso a una única persona de forma individual e intransferible.	
RCA006	En los dispositivos provistos por la entidad/operador que utilicen teclados físicos (PIN PAD) o teclados virtuales (imagen en pantalla) para el ingreso del factor basado en algo que sabe, el valor ingresado debe ser encriptado inmediatamente después de su ingreso mediante un algoritmo no menor a: a. 3DES para dispositivos que permitan transacciones establecidas con criticidad de nivel 1 en los escenarios del punto 6.5. b. DES para dispositivos que permitan transacciones establecidas con criticidad de nivel distinto a 1 en los escenarios del punto 6.5.	A partir del 01/03/2013, es aplicable a nuevas adquisiciones/desarrollos, reemplazos o actualizaciones de dispositivos/aplicaciones provistos por la entidad/operador.
RCA007	Los sistemas de acceso y verificación de credenciales de los CE contemplados en el escenario descripto, deben garantizar la no reutilización del último valor generado de los elementos de autenticación basados en el factor "algo que sabe" .	
RCA008	La caducidad de los elementos de autenticación basados en "algo que sabe", debe establecerse según el análisis de riesgo de cada entidad o al vencimiento del factor basado en "algo que tiene" asociado al canal, cuando aplique. No obstante, las entidades financieras deben implementar los mecanismos necesarios para que los clientes bancarios puedan voluntariamente realizar el cambio aún antes de ese plazo, así como prevenir su presentación luego de vencido el plazo que determina la validez de los mismos.	
RCA009	Los elementos de autenticación basados en el factor "algo que tiene", siempre que empleen mecanismos de autenticación dinámica (Token, tarjeta de coordenadas, entre otros), deben poseer al menos dos de las siguientes características: a. Mecanismos que impidan su duplicación o alteración (Anti tampering). b. Control de relación unívoca entre cliente/cuenta y dispositivo. c. Identificación única de fabricación. d. Recambio bianual.	
RCA010	Las entidades/operadores, deben aplicar técnicas de protección, según su análisis de riesgo que minimicen la exposición de los factores de identificación y autenticación basados en "algo que tiene", cuando los mismos sean presentados ante dispositivos o medios que revelen a terceros datos confidenciales o códigos de seguridad de las credenciales, en operatorias no presenciales (Internet, WebPos, Venta Telefónica, dispositivos desatendidos), considerando pero no limitándose a las siguientes técnicas: a. Uso de esquemas de verificación complementaria por vías seguras (segundo factor, secretos compartidos, técnicas consideradas en el requisito RCA040). b. Valores aleatorios de identificación de TD/TC (PAN o CVC/CVV variable).	

Tabla de requisitos de Control de Acceso (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
RCA011	Debe limitarse la exposición de los datos identificatorios de las credenciales a aquellos usuarios autorizados por la entidad/operador que por necesidades de uso/conocimiento se encuentren calificados para el acceso a esta información.	
RCA012	En la etapa de inicio de sesión/presentación de credenciales, las entidades/operadores, deben ejecutar acciones específicas para proteger la fortaleza de los factores de identificación y autenticación empleando optativamente: a. Dos factores de autenticación de distinto tipo (autenticación fuerte), en alguna de las combinaciones: "algo que tiene" y "algo que sabe", "algo que sabe" y "algo que es" o,"algo que tiene" y "algo que es". b. Dos factores de autenticación del mismo tipo (autenticación simple), dónde uno de ellos identifique de forma unívoca al usuario.	
RCA013	En caso de falla o indisponibilidad total o parcial de los mecanismos de seguridad (Control de Acceso, Monitoreo, Integridad y Registro) en el dispositivo provisto por la entidad/operador, debe mantenerse inhabilitado totalmente el mismo, informando y previniendo al usuario para que evite la presentación de credenciales y la recepción o entrega de valores.	
RCA014	Los elementos de autenticación basados en el factor "algo que sabe", utilizados en el CE, deben poseer una longitud no inferior a 8 caracteres para BI, 6 caracteres para BM y 4 caracteres para BT.	
RCA015	Los elementos de autenticación basados en el factor "algo que sabe" y sean estrictamente "numéricos" deben: a. Limitarse a elementos del tipo PIN ("Personal Identification Number"). b. Poseer una longitud mínima de 4 dígitos.	
RCA016	Durante todo el ciclo de las tareas asociadas al escenario, los datos y credenciales de un cliente no deben estar en posesión completa de una misma persona o grupo de personas o ser asociados a los datos del cliente salvo por los clientes mismos.	
RCA017	Los elementos de autenticación basados en el factor "algo que sabe" durante sus procesos de generación, uso y transporte deben encontrarse protegidos por medio de alguna de las siguientes técnicas: a. Encripción no menor a 3DES. b. Digesto irreversible o funciones de "hashing". En BT, cuando no se utilice alguna de las técnicas descriptas, se debe garantizar que el mecanismo de autenticación del factor sea distinto al empleado para otros CE de un mismo cliente y entidad financiera.	A partir del 01/03/2013 es aplicable a nuevas adquisiciones/desarrollos, reemplazos o actualizaciones de dispositivos/aplicaciones provistos por la entidad/operador.
RCA018	Los elementos de autenticación basados en el factor "algo que sabe" deben limitar su exposición durante el ingreso o reproducción, en los procesos de generación, renovación y uso, considerando, pero no restringiéndose a la implantación alternativa de: a. Máscaras visuales en la pantalla de dispositivos provistos por la entidad/operador. b. Teclados virtuales en aplicaciones provistas por la entidad/operador. c. Paneles protectores de visualización en los dispositivos provistos por la entidad/operador (ejemplo: PCI PIN - Security Requirement 2.0).	
RCA019	Los procesos de generación de los elementos de identificación y autenticación basados en el factor "algo que tiene" deben realizarse en un esquema de separación de funciones tal, que impida que se combinen con la generación de los elementos de identificación y autenticación basados en el factor "algo que sabe". Ejemplos: embozado de tarjetas y generación de PIN; la instancia de sincronización de un token está diferenciada de su distribución.	
RCA020	Los elementos de identificación y autenticación basados en TD/TC deben contar al menos con las siguientes características: a. Nombre y apellido del cliente bancario. b. Número interno de inscripción (número de tarjeta). c. Firma hológrafa o manuscrita. d. Fecha de vigencia. e. Fecha de vencimiento. f. Número de atención de denuncias.	A partir del 01/03/2013 y sólo para renovaciones y nuevas TD/TC.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de requisitos de Control de Acceso (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
RCA021	Los procesos de distribución de elementos de identificación y autenticación, basados en el factor "algo que tiene" deben garantizar la identificación positiva del titular antes de su entrega.	
RCA022	Los elementos de identificación y autenticación basados en el factor "algo que tiene", luego de su retención, deben tener una vigencia no mayor a 30 días hábiles para su descarte o desvinculación del cliente y sus cuentas en forma posterior al tiempo determinado en caso de no ser devueltos al cliente.	
RCA023	Los elementos de autenticación basados en el factor "algo que sabe" y "algo que es" deben bloquear el acceso al CE luego de no más de cinco intentos fallidos consecutivos de inicio de sesión, informar al usuario mediante el esquema implementado de alertas tempranas (RCA041) y aplicar un mecanismo de autenticación positiva para el desbloqueo dentro de los considerados en el requisito RCA040. Luego de un tiempo no mayor a 30 minutos desde el último intento fallido registrado, salvo casos de bloqueo, podrá reiniciarse el registro de intentos fallidos.	
RCA024	En caso de falla o indisponibilidad parcial o total de los mecanismos de seguridad (Control de Acceso, Monitoreo, Integridad y Registro) en el servicio provisto por y desde la entidad/operador, debe mantenerse inhabilitado totalmente el servicio, informando y advirtiendo al usuario para que evite la presentación de credenciales desde un dispositivo propio.	
RCA025	En los dispositivos provistos por la entidad/operador que acepten el ingreso (mecanismo de tracción) de TD/TC, y que por falla mecánica u olvido del usuario retuvieran una TD/TC en el dispositivo, la entidad/operador debe proceder a la devolución al titular de la TD/TC o en caso de no hacerse efectiva, a su destrucción en un tiempo no mayor a 10 días hábiles posteriores a su extracción en los procesos de balanceo o mantenimiento del dispositivo.	
RCA026	En todos los casos de factores de autenticación basados en "algo que sabe" que hayan sido generados por la entidad/operador, se deben implementar mecanismos para asegurar que el cliente bancario modifique los valores generados en su primera presentación ante el CE. Dicho cambio, puede efectuarse mediante un CE distinto del considerado en el escenario, siempre que utilice autenticación fuerte.	
RCA027	En todos los casos de factores de identificación de usuarios generados por la entidad/operador se debe ofrecer al usuario la posibilidad de modificar dicho valor a uno elegido por el usuario.	
RCA028	Los elementos de autenticación basados en el factor "algo que sabe", utilizados para el ingreso al CE, deben poseer una composición alfanumérica y una complejidad tal, que incluya al menos la combinación de tres de los siguientes atributos: a. Caracteres especiales. b. Letras mayúsculas. c. Letras minúsculas. d. Números. e. No contener más de dos caracteres alfanuméricos iguales y consecutivos. f. Estar compuestas por datos no triviales (se descartan: números de teléfono, nombres propios, entre otros). Solamente en los canales BM y BT podrán establecerse caracteres exclusivamente numéricos, con una complejidad tal que se prevenga la selección de: g. Serie de caracteres del mismo número. h. Incremento o decremento de número consecutivo.	
RCA029	Los elementos de autenticación de las credenciales basadas en el factor "algo que sabe" y empleados en el inicio de sesión del CE, deben prevenir estar asociadas a datos personales públicos del cliente bancario o de la entidad financiera.	
RCA030	La suscripción a un CE debe realizarse para su aprobación desde un medio que utilice identificación positiva de acuerdo con las técnicas descriptas en el requisito RCA040.	
RCA031	La generación y renovación del PIN asociado a una TD/TC basada en banda magnética según el RCA044 punto a, debe garantizar un valor diferente entre los canales ATM y POS, siempre que se utilice un PIN asociado a una misma TD/TC.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de requisitos de Control de Acceso (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
RCA032	La entidad/operador debe ejecutar las siguientes acciones para la protección de las transacciones involucradas en el escenario: a. En el caso de aplicar en la etapa de inicio de sesión/presentación de credenciales, alguna de las técnicas descriptas en el requisito RCA012 punto a. y antes de la confirmación de una transacción de banca individual o grupo interrelacionado de transacciones de banca comercial, debe aplicar técnicas de autenticación complementarias para revalidar la identidad del usuario autorizado, entre las que se incluyen pero no se limitan: secretos compartidos, mecanismos de autenticación simple, rellamada o uso de canal alternativo. b. En el caso de aplicar en la etapa de inicio de sesión/presentación de credenciales, la técnica descripta en el requisito RCA012 punto b. y antes de la confirmación de una transacción de banca individual o grupo interrelacionado de transacciones de banca comercial, debe aplicar alguna de las técnicas descriptas en el requisito RCA012 punto a. para revalidar la identidad del usuario autorizado entre las que se incluyen pero no se limitan: usb tokens, token con generación de contraseña o tarjetas de coordenadas. c. Posterior a la confirmación de la transacción y sólo cuando se superen patrones predeterminados en sus sistemas de monitoreo transaccional, debe aplicar al menos una de las técnicas descriptas en el requisito RCA040. Para el canal ATM, cuando se opere mediante uso de tarjeta con circuito integrado (CHIP) bajo estándar EMV y siempre que se satisfaga el cumplimiento del requisito RCA012 punto a, no será exigible el cumplimiento del punto a del requisito RCA032.	
RCA033	La información referida a mecanismos implementados por una entidad/operador para la seguridad del CE y que sea pieza esencial en la protección del mismo, debe conservarse protegido ante la exposición de su contenido a personas no autorizadas.	
RCA034	Los procesos de implementación, prueba y homologación de dispositivos provistos por la entidad/operador y/o aplicaciones específicas para dispositivos no provistos por la entidad/operador para el uso del CE, cuando lo requieran, sólo podrán utilizar credenciales bajo administración de la entidad/operador, no relacionadas con clientes bancarios y no habilitadas para entornos productivos.	
RCA035	Las piezas de software provistos por la entidad/operador para el uso del CE por medio de un dispositivo propio del cliente, no podrán comprometer la privacidad de estos ni de los datos del cliente contenidos en los mismos aun cuando medie autorización del cliente.	
RCA036	Los dispositivos provistos por la entidad/operador deben contar con características físicas que reduzcan la copia, obstrucción, visualización de terceros o retención ilegal de credenciales y valores monetarios, considerando pero no limitándose a la aplicación alternativa de: a. Detectores de objetos adosados a dispositivos provistos por la entidad/operador. b. Mecanismos de información explícita al usuario de las características del dispositivo provisto por la entidad/operador. c. Componentes anti-skimming en el ingreso de credenciales. d. Mecanismos de detección de apertura, violación o alteración de las condiciones físicas del dispositivo (“tampering detection”).	
RCA037	Deben estar descriptos los grupos, roles y responsabilidades para la administración lógica de los componentes de la red de servicios de cada CE.	
RCA038	Los elementos de identificación/autenticación basados en Tarjetas de Débito/Crédito, deben contar con las siguientes características de protección complementaria: a. Impresión de datos de la Tarjeta en bajo o sobre relieve u otra técnica que garantice la legibilidad de los datos identificatorios por al menos el tiempo de vigencia inscripto en la Tarjeta. b. Inclusión de hologramas, códigos de seguridad, entre otros. c. La identificación del emisor y de la entidad bancaria interviniente. d. Los medios de almacenamiento de datos en la Tarjeta (banda magnética, chip, entre otros), no deben almacenar datos completos o legibles de los factores de autenticación.	A partir del 01/03/2013 y sólo para renovaciones y nuevas TD/TC.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de requisitos de Control de Acceso (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
RCA039	En un dispositivo/aplicación asociado a un CE en el que se utilice un mecanismo de autenticación dinámica (token, softtoken, tarjeta de coordenadas, entre otros) y que permita la ejecución de transacciones financieras consideradas en los escenarios con nivel de criticidad 1 de prefijo ETR, los valores generados para componer las "claves dinámicas", deben satisfacer cómo mínimo las siguientes características durante la petición, validación e ingreso de los valores solicitados: a. La clave dinámica debe poseer una estructura no menor a 4 dígitos numéricos aleatorios. b. Los valores de la clave dinámica generados en cada petición, deben tener una vigencia máxima de 120 segundos o hasta su autenticación, lo que ocurra primero. No se exigirá la vigencia por tiempo cuando la entidad/operador asegure que en la ejecución de transacciones financieras consideradas en los escenarios de prefijo ETR con nivel de criticidad 1, la sesión de un CE emplea un valor nuevo y diferente generado por el dispositivo de autenticación dinámica, tanto en la etapa de "inicio de sesión/presentación" como en la de "confirmación" durante una misma sesión. c. Los valores de la clave dinámica generados en cada petición, no deben ser conocidos antes de su generación y durante el proceso de ingreso y validación de los datos por otros individuos distintos del cliente bancario. d. Debe asegurarse una validación del valor generado que garantice su autenticidad estableciendo una correspondencia efectiva del valor generado en el dispositivo/aplicación con el resto de las credenciales del usuario que forman parte del proceso de autenticación. Por ejemplo mediante una sincronización temporal con los sistemas de autenticación del CE, o por comparación univoca de la semilla de generación. e. Las claves dinámicas tienen validez por única vez en una sola transacción de banca individual y un único grupo de transacciones interrelacionadas en la banca comercial. f. Los procesos de autenticación de la clave dinámica deben ocurrir en línea.	
RCA040	La identificación positiva incluye, pero no se restringe a la utilización combinada o no de las siguientes técnicas: a. Cuestionarios predefinidos con presentación aleatoria, con validación automática del sistema. b. Presentación de documentos de identidad emitidos por autoridad nacional que permitan la comparación y convalidación efectiva de las características del portador. c. Firmas holográficas comparables con registro electrónico. d. Identificación ante canal electrónico alternativo con doble factor de autenticación.	
RCA041	Las entidades/operadores deben poner a disposición de sus clientes la siguiente información, estableciendo mecanismos efectivos de alerta en un tiempo no mayor a 24 horas posteriores a la transacción/sesión y de acuerdo a las características de cada CE, sin perjuicio de incluir información adicional acorde con aquella generada por sus sistemas de monitoreo transaccional: a. Fecha y hora de la última transacción/sesión confirmada en el CE. b. Aviso de vencimiento de las credenciales con una antelación no menor al tiempo operativo necesario para su cambio/reposición. c. Nombres del usuario de la sesión y del titular de la cuenta accedida. d. Datos de contacto del servicio al cliente para reporte de irregularidades/consultas.	
RCA042	Las entidades/operadores deben asegurar que los enlaces/accesos desde sesiones de los CE a sitios no bancarios y/o servicios de un tercero que permitan el acceso y ejecución de transacciones bancarias consideradas en los escenarios del punto 6.5. con prefijo ETR, garanticen el cumplimiento de los mismos requisitos establecidos para el CE y no compartan datos confidenciales de las credenciales con los sitios y servicios del tercero.	
RCA043	Los elementos de identificación y autenticación basados en el factor "algo que tiene" luego de su generación y que permanezcan sin entrega efectiva a su destinatario por más de 90 días, deben: a. Descartarse o reasignarse a otro cliente bancario, en el caso de elementos de autenticación dinámica (tokens, tarjetas de coordenadas, entre otros). b. Descartarse en el caso de TD/TC.	

Tabla de requisitos de Control de Acceso (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
RCA044	Los elementos de identificación y autenticación basados en el factor "algo que tiene" deben contar con códigos de seguridad renovables, diferentes en cada renovación de TD/TC y aplicarse a las transacciones contempladas en los escenarios del punto 6.5. bajo prefijo ETR, de la siguiente forma: a. En TD/TC basadas en banda magnética, deben contar un código de verificación de la credencial no visible y almacenado en la banda (ejemplo: CVV1/CVC1) y un código de verificación de la transacción visible (ejemplo: CVV2/CVC2/CID) impreso en la TD/TC. Opcionalmente y sólo para transacciones cursadas de forma presencial (dispositivo físico POS) podrá sustituirse la implementación del código de seguridad de transacción visible en la TD/TC con algún factor de autenticación del tipo "algo que sabe" o PIN en los términos del requisito RCA031. b. En TD/TC basadas en el uso de circuito integrado (chip) o una combinación de este con otras técnicas, deben contar con un mecanismo de autenticación dinámica y un cifrado de los datos almacenados en el circuito integrado. Puede complementarse con un algún factor de autenticación del tipo "algo que sabe" o PIN en los términos del requisito RCA031.	
RCA045	Las entidades/operadores deben considerar, según sus análisis de riesgo, un reemplazo periódico de los elementos de identificación y autenticación basados en "algo que tiene, por nuevos elementos renovados en sus códigos de seguridad aplicando, por ejemplo, los siguientes criterios: a. Ante las siguientes situaciones presentadas por el tenedor: 1. Denuncia de robo, pérdida o deterioro. 2. Desconocimiento de transacciones efectuadas. b. Ante el vencimiento inscripto en un TD/TC con una antelación mínima de 20 días, deshabilitando en forma inmediata la emisión anterior o activación del reemplazo, lo que ocurra primero. c. Ante la detección de una de las situaciones consideradas en el requisito RMC009. d. Ante cambios de diseño, formato o técnicas de elaboración que modifiquen los elementos de seguridad de las TD/TC se debe proceder con un plan de reemplazo con ejecución no mayor al plazo restante para la renovación original. e. Ante la detección de fallas de fabricación o pérdida durante la distribución y/o almacenamiento. debe procederse al descarte, reemplazo y renovación de todas las TD/TC involucradas. Asimismo, las entidades deben considerar una migración paulatina de las TD/TC a tecnología de microcircuito integrado favoreciendo la expansión del mercado, la seguridad transaccional, la interoperabilidad y la evolución de los servicios financieros.	
RCA046	Las TD/TC basadas en circuito integrado (CHIP) según lo indicado en el requisito RCA044 y que además cuenten con banda magnética (Sistema Dual), no podrán formalizar transacciones mediante el uso de banda magnética cuando la terminal POS o ATM cuente con lector de CHIP habilitado salvo excepciones que deberán quedar con un registro diferenciado y formar parte de los análisis del punto RMC009.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de requisitos de Control de Acceso (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
RCA047	En la utilización de TD/TC basadas en circuito integrado (CHIP) bajo estándar EMV, y según el método de autenticación elegido, las entidades y operadores deben: a) Para TD/TC que utilicen el método de autenticación, basados en la verificación de en un dato estático o firma grabada en el CHIP (SDA -Static Data Authentication por sus siglas en Inglés) las transacciones de los escenarios del punto 6.5. bajo prefijo ETR sólo deberán realizarse en la modalidad "en línea" (ver glosario). Del mismo modo, deberán incorporar un segundo factor de autenticación de acuerdo a lo indicado en el requisito RCA032 cuando las transacciones involucren extracciones, transferencias o pagos de bienes y servicios fuera de los límites del concepto "bajo valor" (ver glosario) b) Para TD/TC que utilicen los métodos de autenticación basados en la generación dinámica de claves de autenticación (DDA/CDA – Dynamic Data Authentication/ Combined Dynamic Data Authenticacion), las transacciones de los escenarios del punto 6.5. bajo prefijo ETR podrán realizarse en las modalidades "en línea" o "fuera de línea". Por otra parte, deberán incorporar un segundo factor de autenticación de acuerdo a lo indicado en el requisito RCA032 cuando las transacciones involucren extracciones, transferencias o pagos de bienes y servicios fuera de los límites del concepto "bajo valor" (ver glosario)	
RCA048	En los componentes lectores provistos o no por la entidad/operador para la lectura del factor "algo que tiene" (TD/TC) vinculados o no a dispositivos móviles o computadores personales, deben satisfacerse los siguientes requerimientos:: a. El valor capturado por el lector, debe ser encriptado desde el lector mediante un algoritmo no menor a 3DES para componentes que permitan transacciones establecidas con criticidad de nivel 1 en los escenarios del punto 6.5. b. El lector debe encontrarse asociado de manera univoca a los siguientes tres elementos: (1) red de procesamiento, dispositivo móvil o computador personal, (2) el servicio provisto por la entidad/operador y el (3) cliente/comercio. c. El lector debe ser homologado por la entidad/operador para la provisión del servicio.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

6.7.3. Tabla de requisitos de Integridad y Registro.

Tabla de requisitos de Integridad y Registro		
Código de requisito	**Descripción de requisito**	**Alcance**
RIR001	Los datos de autenticación de las credenciales no deben ser almacenados en el dispositivo provisto por la entidad/operador ni conservados en el registro de actividad del mismo (Journal).	
RIR002	El registro de las actividades en los sistemas aplicativos y/o dispositivos provistos por la entidad/operador, debe garantizar para cada evento al menos: a. Identificación. b. Descripción. c. Fecha y hora completa. d. Identificación de origen. e. Usuario actor.	
RIR003	Los registros colectados por los sistemas aplicativos y/o dispositivos provistos por la entidad/operador deben asegurar la trazabilidad de las acciones realizadas en la totalidad de las actividades, identificando quién (persona/dispositivo/cuenta/oriogen/destino), qué (actividad/función/transacción), dónde (CE, ubicación), cuándo (tiempo) y cómo (patrón/relación de eventos).	
RIR004	Los registros de los sistemas aplicativos y/o dispositivos provistos por la entidad/operador deben contemplar al menos los siguientes eventos: a. Solicitudes y respuestas a acciones transaccionales y de mantenimiento de las aplicaciones. b. Errores y fallas de la aplicación o el dispositivo. c. Intentos exitosos y fallidos de autenticación. d. Gestión de credenciales (alta, eliminación, modificación y asignación de privilegios). e. Gestión de bases de datos/repositorios (creación, eliminación, modificación y consultas). f. Acciones operativas y de mantenimiento (inicio y cierre de los sistemas, fallas y cambios en la configuración).	
RIR005	Los registros de las actividades de cada CE asociado al escenario deben contar desde el momento de su generación, con mecanismos que permitan verificar que cada registro sea único, responda a una secuencia predeterminada y se mantenga inalterable durante su almacenamiento, transporte y recuperación.	
RIR006	Los registros de las actividades de los dispositivos/aplicaciones provistos por la entidad/operador y de las operaciones transaccionales, deben ser almacenados y custodiados mediante alguno de los siguientes regímenes de almacenamiento: a. En el caso de registros digitalizados (Electronic Journal) deben ser enviados en tiempo real o permanecer almacenados por menos de 24 horas en el dispositivo provisto por la entidad/operador que los generó, cuando aplique, debiendo ser trasladados a ese término a una infraestructura de almacenamiento y custodia. b. En el caso de registros impresos (Tira Journal) deben ser enviados en forma inmediata posterior a cada evento de balanceo y carga del dispositivo provisto por la entidad/operador.	
RIR007	Los registros históricos de las actividades y de las operaciones transaccionales deben conservarse por un término no menor a 6 años. Los soportes de almacenamiento del archivo histórico no deben ser recuperables luego de su descarte.	
RIR008	Los soportes de almacenamiento de los registros de las actividades y de operaciones transaccionales en el dispositivo provisto por la entidad/operador no deben ser recuperables luego de los siguientes situaciones: a. 15 días posteriores al traslado confirmado a la infraestructura de custodia y recuperación. b. El descarte del soporte de almacenamiento en el dispositivo.	
RIR009	Los registros de las actividades de los dispositivos/aplicaciones provistos por la entidad/operador y de las operaciones transaccionales, deben contar con mecanismos de protección que aseguren que sólo podrán ser accedidos por aquellos que corresponda según la necesidad de uso/conocimiento.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de requisitos de Integridad y Registro (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
RIR010	Los dispositivos y/o piezas de software provistas por la entidad/operador para el uso del CE, deben asegurar que satisfacen un ciclo de vida y de desarrollo de sistemas, basado en las siguientes etapas conceptuales: a. Análisis de requerimientos. b. Adquisición/fabricación/desarrollo. c. Prueba y homologación. d. Implementación. e. Operación y mantenimiento. f. Descarte y reemplazo. Asimismo, este ciclo, debe proveer los elementos de seguridad relacionados con, pero no limitados a: g. Requisitos funcionales de seguridad. h. Tipos y características de validación de los datos de entrada. i. Granularidad de las funciones y los registros. j. Niveles de acceso. k. Control de Cambios. l. Actualización y Parches.	
RIR011	Los procesos de homologación de dispositivos y/o piezas de software provistos por la entidad/operador para interactuar con el CE, deben garantizar la verificación de todos los aspectos de diseño, funcionalidad, interoperabilidad y características de seguridad definidos en las etapas de adquisición/fabricación/desarrollo e implementación.	
RIR012	Los procesos de homologación e implementación de piezas de software del CE en dispositivos del cliente bancario, deben realizarse utilizando una verificación formal antes de su habilitación. Asimismo, deben utilizarse métodos de instalación que prevengan la exposición de datos personales, financieros o de las credenciales del cliente.	
RIR013	Deben efectuarse los siguientes controles de integridad de los datos transmitidos: a. Identificación del receptor y cuenta destino. b. Credenciales y cuenta de origen. c. Identificación y composición del mensaje.	
RIR014	En la transmisión de datos de credenciales y transacciones, todo punto de conexión entre una red privada y una red pública debe contar con un Firewall en cada conexión a Internet y entre cualquier zona desmilitarizada y la zona de la red interna, incluida toda red inalámbrica. Aplica solamente a la infraestructura de la entidad/operador que gestiona el CE con redes basadas en TCP/IP.	
RIR015	Cuando el transporte de datos de credenciales y transacciones se realice mediante el empleo de redes públicas y/o parcialmente privadas en alguno de sus tramos, la entidad/operador debe incluir mecanismos de protección del vínculo y la sesión en los CE, incluyendo pero no limitándose a: a. Uso de protocolos seguros para la transmisión de datos (tales como TLS/SSL/IPSEC/SSH) en redes públicas (tales como 3G, 4G/LTE, GSM, GPRS, WIFI, Internet). b. Uso de métodos de protección del sitio bancario (Certificados digitales basado en infraestructura de clave pública). c. cifrado sólido en redes que utilicen protocolos basados en TCP/IP. Este requisito es únicamente aplicable a los canales TAS, POS y ATM y cuando utilicen redes públicas con protocolos basados en TCP/IP.	
RIR016	En todos los casos, los dispositivos/aplicaciones provistos por la entidad/operador, deben poder generar un comprobante de la transacción efectuada que resulte único y verificable contra los registros de actividad del canal. Incluye pero no se limita a la aplicación alternativa de alguna de las siguientes opciones: a. Papel impreso para dispositivos físicos provistos por la entidad/operador. Emitirse a demanda del cliente en caso que no requiera firma del cliente, obligatoriamente cuando requiera firma del cliente, b. Formato digital para dispositivos propios del cliente, recuperable por al menos 3 meses posteriores a la transacción. Adicionalmente, los datos de identificación de las credenciales del cliente deben limitarse a los estricta y mínimamente necesarios y no deben aparecer de forma completa en el comprobante.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de requisitos de Integridad y Registro (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
RIR017	En los procesos de compatibilización de dispositivos y/o implementación de piezas de software en entornos controlados por el usuario, la entidad/operador debe definir e informar al cliente bancario, los requisitos de seguridad aplicables a los dispositivos propios del usuario, realizando las siguientes tareas: a. Informar los criterios de admisibilidad de los dispositivos del usuario, así como las limitaciones de hardware, software, conectividad y entorno para su uso en el CE. b. El CE debe prevenir el acceso a través de un dispositivo que no satisface los criterios de admisibilidad determinados. c. Detectar e informar al usuario las acciones necesarias para mantener habilitado el servicio desde el dispositivo.	
RIR018	Las credenciales basadas en TD/TC que fueran retenidas durante el uso de los dispositivos provistos por la entidad/operador, deben asegurar el cumplimiento de las siguientes acciones operativas: a. Posterior a su retención la entidad/comercio debe informar al emisor antes de transcurridas 24 horas y en el menor tiempo posible de acuerdo con los medios disponibles. b. La entidad/operador emisor debe resolver el incidente en un lapso no mayor a 48 horas. c. En los casos que el material retenido no sea legítimo debe conservarse bajo custodia con los recaudos necesarios para evitar su uso, como material de prueba para posterior investigación.	
RIR019	Las aplicaciones (piezas de software) empleadas para brindar servicios financieros en dispositivos móviles deben garantizar la vinculación única entre la “aplicación”, las credenciales del cliente y el dispositivo móvil, considerando pero no limitándose a las siguientes técnicas combinadas:: a) Asociación de identificador IMEI (International Mobile Station Equipment Identity, por su siglas en inglés) o código único de identificación del dispositivo. b) Semilla para encripción de datos y/o credenciales c) Valor aleatorio que identifica la relación del dispositivo con el servicio financiero. Las aplicaciones para dispositivos móviles deben alojarse en sitios cuyas condiciones de seguridad sean acordes con la política de la entidad financiera y estos ser informados al consumidor de servicios financieros de manera fehaciente.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

6.7.4. Tabla de requisitos de Monitoreo y Control.

Tabla de Requisitos de Monitoreo y Control		
Código de requisito	**Descripción de requisito**	**Alcance**
RMC001	La entidad/operador debe establecer un tiempo máximo de inactividad de la sesión en cada dispositivo/aplicativo provisto al cliente para el uso del CE. Este tiempo debe garantizar que la sesión no permanezca abierta de forma indefinida e incluir pero no limitarse a las siguientes acciones: a. Expiración de la sesión por tiempo establecido para cada canal según análisis de vulnerabilidades documentado. b. Expiración de la sesión en un tiempo no mayor en ningún caso a 30 minutos.	
RMC002	Los dispositivos provistos por la entidad/operador que presenten problemas de comunicación o fallas de funcionamiento total o parcial de los mecanismos de seguridad (Control de Acceso, Integridad y Registro), deben asegurar un monitoreo oportuno basado en alertas y registro de las acciones emprendidas para su inhabilitación/reparación según corresponda.	
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. Este requisito no incluye los dispositivos propios del cliente, ni los elementos de autenticación basados en el factor “algo que tiene” provistos por la entidad/operador.	
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.	
RMC005	Las entidades deben implementar mecanismos de comunicación alternativa con sus clientes con objeto de asegurar vías de verificación variada ante la presencia de alarmas o alertas ocurridas por efecto del monitoreo transaccional implementado.	
RMC006	A partir de los registros colectados por los sistemas aplicativos de la entidad/operador asociados al escenario, se debe realizar una clasificación y determinación de los eventos de seguridad, una definición de los límites y umbrales de compromiso, niveles de comportamiento normal/inesperado y establecer las acciones de acuerdo con cada clasificación y limite determinado.	
RMC007	Los dispositivos provistos por la entidad/operador que interactúen con TD/TC deben contar con mecanismos de alerta en caso de olvido y retención de la TD/TC, con excepción del canal POS.	
RMC008	La entidad financiera debe proveer vías de comunicación para la recepción de consultas/denuncias de los clientes las 24 horas.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de requisitos de Monitoreo y Control (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
RMC009	Los sistemas de monitoreo transaccional de las entidades/operadores de TD/TC, deben asegurar la detección, registro y control de situaciones que establezcan un compromiso de datos sensibles que incluya pero no se limite a las siguientes: a. Punto común de compromiso. punto de venta, adquirente, proveedor, entre otros que comprometan transacciones de TD/TC cursadas por el mismo. b. Fuga de información. Pérdida ocurrida en la infraestructura técnica y/o organizacional de la entidad financiera, operador, adquirente, distribuidor y/o proveedores que comprometa información sensible de las TD/TC (números de tarjeta, códigos de seguridad, datos confidenciales del cliente, entre otros) c. Códigos de Seguridad. Compromiso demostrado de los algoritmos de cálculo de los códigos de seguridad de las TD/TC.	
RMC010	Los dispositivos/aplicaciones provistos por la entidad/operador, deben detectar la apertura simultánea de más de una sesión, para un mismo usuario, canal y entidad financiera, ejecutando una de las siguientes acciones: a. Impedir la apertura simultánea de más de una sesión b. Bloquear la operatoria inmediatamente después de la detección, informando al cliente de la irregularidad. El CE ATM podrá exceptuarse de las acciones indicadas en los puntos a y b siempre que se incluyan en los sistemas de monitoreo y control las configuraciones necesarias para detectar y registrar los eventos indicados en el 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.	
RMC012	El proceso de apertura de los dispositivos para ATM y TAS debe garantizar: a. Ser realizada por dos personas, dejando constancia escrita en un acta de su participación y del resultado de la conciliación, balanceo de billetes, conformidad de depósitos, tarjetas retenidas, totales, diferencias si las hubiera, entre otros. b. En los casos de dispositivos neutrales, la documentación de respaldo (planillas o formularios de balanceo, de reposición, de tarjetas retenidas, de conciliación y otras) debe ser firmada, posteriormente, por un funcionario de la entidad financiera, que será la figura responsable para cualquier intervención posterior ante requerimientos de este Banco Central.	
RMC013	Durante los procesos de mantenimiento, configuración, apertura, carga y balanceo de los dispositivos contemplados en el escenario, con excepción del canal POS, se deben satisfacer las siguientes consignas: a. Debe asegurarse una segregación física y lógica de las siguientes funciones: • Administración (instalación, configuración y ajuste de parámetros en el sistema operativo y aplicativo). Debe encontrarse limitada a personal del operador/entidad responsable del servicio. • Operación (ejecución de tareas operativas de consulta, balanceo y reporte). Debe limitarse a responsables de la entidad o tercero contratado por la entidad para los procesos indicados. • Apertura y cierre de dispositivo y tesoro. Debe aplicarse un control dual para el uso y posesión temporal de las llaves físicas y/o lógicas asegurando que en el proceso participan al menos dos personas donde preferentemente una de ellas debe pertenecer a la entidad. b. Debe asegurarse la puesta en práctica de procedimientos internos de la entidad para el control de la documentación de respaldo de las tareas operativas relacionadas.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

6.7.5. Tabla de requisitos de Gestión de Incidentes.

Tabla de requisitos de Gestión de Incidentes		
Código de requisito	**Descripción de requisito**	**Alcance**
RGI001	Debe realizar con una periodicidad mínima anual y con base en el análisis de riesgo de los activos informáticos asociados al escenario, un análisis de los incidentes ocurridos y un reporte que sirva para establecer medidas de protección, contenidos del programa de capacitación y concientización, modificaciones a la registración y control de eventos, y una redefinición de las alertas, límites y umbrales.	
RGI002	La identificación de incidentes debe estar basada al menos en alertas tempranas, estadísticas de tipo/frecuencia/patrón de incidentes y recomendaciones de seguridad informática.	
RGI003	La gestión de incidentes de seguridad puede ejecutarse en forma descentralizada pero debe ser coordinada con personal de la entidad financiera.	
RGI004	No definido.	
RGI005	Los incidentes detectados deben recibir un tratamiento regular con un escalamiento definido formalmente.”	

Asimismo les hacemos llegar las hojas que, en reemplazo de las oportunamente provistas, corresponde incorporar en las normas de la referencia.

Saludamos a Uds. atentamente.

BANCO CENTRAL DE LA REPÚBLICA ARGENTINA

Mara I. Misto Macias
Gerente Principal de
Seguridad de la Información

Agustín Torcassi
Subgerente General
de Normas

ANEXO

Índice

6.1. Alcance.

Se encuentran alcanzadas las entidades financieras que intervengan en la prestación, por sí o por terceros en su nombre, de servicios financieros por intermedio de algunos de los siguientes Canales Electrónicos (CE), cuya definición y características se encuentra en el Glosario del punto 6.6.:

6.1.1. Cajeros Automáticos (ATM).

6.1.2. Terminales de Autoservicio (TAS).

6.1.3. Banca Móvil (BM).

6.1.4. Banca Telefónica (BT).

6.1.5. Banca por Internet (BI).

6.1.6. Puntos de Venta (POS).

6.1.7. Plataforma de Pagos Móviles (PPM)

6.2. Procesos de referencia.

De modo referencial y con el objetivo de facilitar la implementación de los requisitos de seguridad determinados en esta sección, la Gestión de Seguridad de los Canales Electrónicos se entiende como el ciclo de procesos que reúnen distintas tareas, especialidades y funciones, de manera integrada e interrelacionada, repetible y constante para la administración, planificación, control y mejora continua de la seguridad informática en los Canales Electrónicos.

Los Procesos de Referencia aquí señalados, reúnen el conjunto de tareas y especialidades que las entidades pueden poseer, con estas u otras denominaciones y en la composición orgánica que mejor atienda sus intereses y satisfaga las funcionalidades y propósitos descriptos. Asimismo, deben informar a la Gerencia de Auditoría Externa de Sistemas la estructura e interrelaciones orgánicas y operativas que en sus organizaciones se corresponda:

6.2.1. Concientización y Capacitación (CC).

Proceso relacionado con la adquisición y entrega de conocimiento en prácticas de seguridad, su difusión, entrenamiento y educación, para el desarrollo de tareas preventivas, detectivas y correctivas de los incidentes de seguridad en los Canales Electrónicos.

6.2.2. Control de Acceso (CA).

Proceso relacionado con la evaluación, desarrollo e implementación de medidas de seguridad para la protección de la identidad, mecanismos de autenticación, segregación de roles y funciones y demás características del acceso a los Canales Electrónicos.

6.3.1.4. Los errores de encuadramiento detectados por las auditorías internas y/o externas obligan a las entidades a efectuar los ajustes correspondientes en un plazo no mayor a 180 días corridos posteriores a su notificación, debiendo presentar a la Superintendencia de Entidades Financieras y Cambiarias, un informe de las adecuaciones efectuadas avalado por una verificación de conformidad de su Auditoría Interna, posterior al vencimiento de plazo indicado. La Superintendencia de Entidades Financieras y Cambiarias podrá realizar una verificación de lo actuado

6.3.2. Del cumplimiento de los requisitos técnico-operativos mínimos.

6.3.2.1. Las entidades deben desarrollar, planificar y ejecutar un plan de protección de sus activos, procesos, recursos técnicos y humanos relacionados con los Canales Electrónicos bajo su responsabilidad, basado en un análisis de riesgo de actualización periódica mínima anual, en su correspondencia con la Matriz de Escenarios y en los requisitos técnico-operativos detallados en los puntos 6.7. y subsiguientes.

6.3.2.2. Dentro de las tareas de gestión de la seguridad, e independientemente del área, personas o terceros que tengan a su cargo la función y la ejecución de las tareas, las entidades deben contar con funciones y tareas relacionadas con los siguientes procesos estratégicos de seguridad para sus Canales Electrónicos:

6.3.2.2.1. Concientización y Capacitación. Complementariamente a lo indicado en el punto 6.2.1., las entidades deben contar con un programa de concientización y capacitación de seguridad informática anual, medible y verificable, cuyos contenidos contemplen todas las necesidades internas y externas en el uso, conocimiento, prevención y denuncia de incidentes, escalamiento y responsabilidad de los Canales Electrónicos con los que cuentan.

6.3.2.2.2. Control de Acceso. Complementariamente a lo previsto en el punto 6.2.2., 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.

6.3.2.2.3. Integridad y Registro. Complementariamente a lo indicado en el punto 6.2.3., 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.

6.3.3.4. Con el objeto de que este Banco Central pueda analizar los alcances particulares, y características técnicas, para eventuales recomendaciones de seguridad informática, con anterioridad a su implementación, las entidades financieras, deberán informar sobre cualquier nuevo Canal Electrónico no contemplado en el punto 6.1. o modalidad operativa diferente de las contempladas en esta sección.

6.3.3.5. Las propuestas de implementación de un nuevo CE o modalidad diferente de las contempladas en esta sección, previo un análisis de riesgo de la entidad financiera, deben ser informadas al menos con 60 días de anticipación a la Gerencia Principal de Seguridad de la Información, para que en conjunto con la Gerencia Principal de Sistemas de Pago y Cuentas Corrientes analicen los alcances particulares, características técnicas e impacto de la implementación y de corresponder brinden las eventuales recomendaciones que consideren necesarias o realicen los ajustes normativos que correspondiesen.

6.3.3.6. En todos aquellos casos en que la operación no esté asociada a una clave de identificación personal, ante el desconocimiento por parte del cliente de una transacción efectuada mediante POS o PPM, las entidades financieras deben proceder a la inmediata devolución/acreditación de los fondos al cliente, sin perjuicio de iniciar la investigación de la operación y eventualmente, las acciones administrativas y/o legales que correspondieran.

6.4. Escenarios de Canales Electrónicos.

6.4.1. Guía.

Cada escenario está compuesto por: una categoría de agrupación temática, una situación considerada dentro de la categoría, una determinación de la aplicabilidad del escenario en los Canales Electrónicos considerados, un valor de criticidad que indica la importancia relativa del escenario y que afecta los requisitos mínimos considerados y, finalmente, un conjunto de requisitos técnico-operativos para controlar la situación descripta.

Un escenario se presenta como una fila dentro de la matriz. Se utilizan tres categorías, que agrupan los principales escenarios de interés:

- Credenciales y Medios de Pago (CM). Se refiere a los elementos dispuestos para la identificación, autenticación y autorización de acceso/uso de los medios y dispositivos de los Canales Electrónicos. Se incluyen aquellos 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). Se refiere a las características de los dispositivos y piezas físicas y lógicas intervinientes en la operación de los Canales Electrónicos respectivos.

- Transacciones (TR). Se refiere a la naturaleza de las operaciones financieras, operativas y de consulta que permita realizar el Canal Electrónico.

Las situaciones describen el escenario particular sujeto a tratamiento y para el que se han determinado requisitos técnico-operativos mínimos particulares.

La aplicabilidad se encuentra determinada para los Canales Electrónicos considerados en la norma y en el escenario en particular. No a todos los canales les aplica el mismo escenario descripto.

6.4.2. Criticidad y Cumplimiento.

La criticidad es un ponderador que establece el nivel de importancia relativo de un escenario y sus necesidades regulatorias. Las entidades deben instrumentar los mecanismos necesarios para considerar la aplicabilidad del escenario a su contexto particular y su inclusión en la matriz de riesgo operacional de tecnología que emplee en su gestión de riesgo operacional acorde con lo indicado en los puntos 6.4.1. y subsecuentes.

El nivel de obligación de las entidades de cumplir los requisitos técnico-operativos está determinado por tres elementos: la criticidad asignada, la vigencia determinada en cada requisito técnico-operativo y los resultados de la gestión de riesgo de las entidades financieras.

Los valores de criticidad, los criterios utilizados para su asignación a cada escenario y el cumplimiento se determinan según lo indicado en la siguiente tabla.

Valor	Descripción	Criterios de asignación	Cumplimiento
1	Alta exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma extendida la disponibilidad de los servicios y la confiabilidad de el/los CE, la entidad financiera y el sistema financiero en general.	• Exposición al riesgo sistémico y propagación del efecto negativo. • Impacto económico sobre los clientes y la entidad financiera. • Nivel de penetración del Canal Electrónico y Medio de Pago asociado. • Interoperabilidad y efectos sobre otros CE.	Obligatorio. Las entidades financieras deben satisfacer los requisitos técnico operativos de cada escenario de acuerdo con la Tabla de Requisitos correspondiente (punto 6.7).
2	Moderada exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma limitada la disponibilidad y la confiabilidad de el/los CE involucrados, la entidad financiera y el sistema financiero en general.		Alineado. Las entidades deben realizar sus mejores esfuerzos para satisfacer los requisitos técnico-operativos de cada escenario, implementando medidas compensatorias y/o alternativas en aquellos requisitos que no satisfagan los indicados en la Tabla de Requisitos correspondiente (punto 6.7).
3	Baja exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma limitada la disponibilidad y la confiabilidad en el/los CE involucrados, la entidad financiera o el sistema financiero en general.		Esperado. Las entidades podrán satisfacer los requisitos de acuerdo con los resultados formales de su gestión de riesgo

La asignación de los valores en cada escenario, es una potestad de este Banco Central. No obstante, cuando no se encuentre asignado un valor a un determinado escenario, las entidades financieras deben asignarlo siguiendo los criterios establecidos en la tabla y los resultados formales de su gestión de riesgo operacional. Este Banco Central queda facultado para realizar actualizaciones periódicas de estos valores, adecuando los mismos de acuerdo con el resultado de sus verificaciones, el comportamiento del sistema financiero y el contexto nacional.

6.5. Matriz de Escenarios.

Matriz de Escenarios					
Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
Credenciales y Medios de Pago	ECM001	Generación, distribución y descarte de credenciales que incluyen TC/TD.	ATM; TAS y POS.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC010; RCC013; RCC014; RCA001; RCA003; RCA009; RCA011; RCA012; RCA015; RCA016; RCA017; RCA018; RCA019; RCA020; RCA021; RCA031; RCA037; RCA038; RCA043; RCA044; RCA045; RIR002; RIR003; RIR005; RIR009; RGI001; RGI002; RGI003 y RGI005.
	ECM002	Generación, distribución y descarte de Credenciales que no incluyen TC/TD.	BI; BM; PPM y BT.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC010; RCC013; RCC014; RCA001; RCA003; RCA009; RCA011; RCA012; RCA014; RCA016; RCA017; RCA018; RCA019; RCA028; RCA029; RCA037; RCA043; RIR002; RIR003; RIR005; RIR009; RGI001, RGI002; RGI003 y RGI005.
	ECM003	Suscripción, presentación, uso, renovación y baja de credenciales que incluyen TD/TC.	ATM; TAS; PPM y POS.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC013; RCC014; RCA002; RCA003; RCA004; RCA005; RCA006; RCA007; RCA008; RCA009; RCA010; RCA011; RCA012; RCA013; RCA015; RCA017; RCA018; RCA022; RCA023; RCA025; RCA026; RCA030; RCA031; RCA036; RCA040; RCA041; RCA044; RCA045; RCA048; RIR001; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR015; RIR016; RMC005; RMC006; RMC007; RMC008; RMC009; RMC010; RGI001, RGI002; RGI003 y RGI005.
	ECM004	Suscripción, presentación, uso, renovación y baja de credenciales sin TD/TC.	BI; BM; PPM; TAS y BT.	**1**	RCC001; RCC002; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCC014; RCA002; RCA003; RCA004; RCA005; RCA007; RCA008; RCA009; RCA010; RCA011; RCA012; RCA014; RCA017; RCA018; RCA022; RCA023, RCA024; RCA026; RCA027; RCA028; RCA030; RCA039; RCA040; RCA041; RCA042; RIR001; RIR002; RIR003; RIR004; RIR005; RIR007; RIR009; RIR015; RIR016; RMC001; RMC005; RMC006; RMC008; RMC010; RGI001, RGI002; RGI003 y RGI005.

Matriz de Escenarios (continuación)

Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
Dispositivos/Aplicaciones	EDA001	Diseño, funcionalidad y homologación de dispositivos suministrados por la entidad o el operador.	ATM; POS y TAS.		RCC006; RCC012; RCC010; RCC013; RCA020; RCA033; RCA034; RCA036; RCA037; RCA038; RIR001; RIR002; RIR003; RIR004; RIR005; RIR009; RIR010 y RIR011.
	EDA002	Compatabilización de dispositivos propios del usuario.	BI; BT; PPM y BM.	**2**	RCC006; RCC010; RCC011; RCC013; RCA034; RCA035; RCA037; RIR012; RIR017 y RIR019.
	EDA003	Diseño, funcionalidad y homologación de aplicaciones para la interacción del usuario con el CE, suministrados por la entidad/operador.	BI; BT; PPM y BM.		RCC006; RCC010; RCC012; RCC013; RCA027; RCA033; RCA034; RCA037; RIR001; RIR002; RIR003; RIR004; RIR005; RIR009; RIR010; RIR011; RIR012 y RIR017.
	EDA004	Operaciones y mantenimiento de dispositivos/aplicaciones con manejo físico de valores.	ATM; TAS y POS.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC009; RCC010; RCC012; RCC013; RCA012; RCA013; RCA015; RCA018; RCA023; RCA026; RCA033; RCA037; RCA040; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR010; RIR014; RIR015; RIR018; RMC003; RMC006; RMC007; RMC009; RMC010; RMC012; RMC013; RGI001; RGI002; RGI003 y RGI005.
	EDA005	Operaciones y mantenimiento de dispositivos/aplicaciones sin manejo físico de valores.	BI; BT; PPM y BM.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC009; RCC010; RCC012; RCC013; RCA012; RCA013; RCA014; RCA018; RCA023; RCA026; RCA033; RCA037; RCA040; RIR002; RIR003; RIR004; RIR005; RIR007; RIR009; RIR010; RIR014; RIR015; RMC001; RMC003; RMC006; RGI001; RGI002; RGI003 y RGI005.

Matriz de Escenarios (continuación)

Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
Transacciones	ETR001	Depósito de valores físicos en el CE con destino directo a cuentas bancarias o pagos de bienes y servicios.	ATM y TAS.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC013; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC006; RMC008; RMC009; RGI001; RGI002; RGI003 y RGI005.
	ETR002	Extracción de efectivo por CE.	ATM.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC013; RCA032; RCA040; RCA046; RCA047 RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR003	Pago de bienes o servicios.	ATM; TAS; POS; BI; BM; PPM y BT.	**2**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR004	Transferencias de fondos entre cuentas de un mismo titular y misma entidad financiera.	ATM; TAS; BI; BM y BT.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR005	Transferencias Inmediatas.	ATM ; BM y BI.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR006	Transferencias ordinarias	ATM; TAS; BI y BM.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR007	Solicitud, formalización y acreditación de operaciones de crédito.	ATM; TAS; BI y BM.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR008	Transacciones de consulta, instrucción operativa o instrucción financiera con confirmación por vía tradicional.	ATM; TAS; BI; BT y BM.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC006; RMC008; RMC009; RGI001; RGI002; RGI003 y RGI005.
	ETR009	Nuevas operatorias transaccionales no contempladas en otros escenarios, con o sin movimiento de fondos.	ATM; TAS; POS; BI; BT; PPM y BM.	**2**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032, RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR010	Transacciones de Bajo Valor: extracciones de efectivo, pago de bienes y/o servicios y transferencias inmediatas.	ATM; POS; BI; BM y PPM	**2**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003; RGI005.

6.6. Glosario de términos utilizados en la Sección 6.

Se incluye, en orden alfabético, la definición aplicable a los términos y acrónimos utilizados en esta sección con objeto de facilitar la interpretación y ofrecer mayor claridad a los contenidos.

Activo. Comprende a los recursos, personas y medios indispensables para la ejecución de uno o más procesos de negocios que sean relevantes en los resultados esperados de estos últimos.

Autenticación Fuerte - Doble Factor. Comprende la utilización combinada de dos factores de autenticación, es decir dos elementos de las credenciales de distinto factor. Complementariamente, considérese lo expuesto sobre **Factores de Autenticación** y **Credenciales**.

Banca Electrónica. Comprende a todo servicio bancario y/o financiero, ofrecido por una entidad y basado en el uso de tecnología para la ejecución de operaciones y transacciones por parte de un usuario de servicios financieros, con mínima o ninguna asistencia o participación de un operador humano. La Banca Electrónica incluye pero no se limita a la implementación de Canales Electrónicos con las características indicadas en esta norma.

Banca Móvil (BM). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros, que se basan en la utilización de aplicaciones (programas) informáticas diseñadas para su implementación y operación en dispositivos móviles propios 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) y se comunican, 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.

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 propios del usuario, 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 datos bajo administración de un operador público o privado.

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.

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.

Cliente - usuario de servicios financieros - usuario. Los términos "cliente" y "usuario de servicios financieros" son equivalentes y se refieren a la persona física o jurídica que se encuentra identificada y suscrita a los servicios de una o más entidades financieras. El término "usuario" es una denominación genérica aplicable a clientes y no clientes.

Contramedidas. Comprende a todas las acciones, planes, tareas operativas, mecanismos de software o hardware dispuestos para mitigar el riesgo de ocurrencia de ataque o compromiso de una vulnerabilidad conocida.

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 dispositivo (factor basado en "algo que tiene").

Control dual. Comprende al proceso que 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. Complementariamente, considérese lo expuesto sobre **Factores de Autenticación**.

Datos personales públicos. Comprende a 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, así como otros usuarios calificados para el mantenimiento y control en sitio. Incluye los elementos lógicos y/o aplicaciones necesarios para brindar funcionalidad y operación a los elementos físicos.

Encripción - métodos. Comprende a los métodos para el cifrado de información con el propósito lograr confidencialidad de su contenido y limitar su revelación a la aplicación de un mecanismo de descifrado previsto. Algunos métodos considerados en esta norma, incluyen, pero no se limitan a DES ("Data Encryption Standard"), 3DES (triple cifrado del DES), entre otros.

Escalamiento - Escalamiento de incidentes. Comprende al protocolo formal y procedimientos específicos para el flujo de ejecución e informe de las actividades de recepción, diagnóstico, análisis, contención, corrección y reporte de los incidentes de seguridad en los Canales Electrónicos.

Evento de seguridad. Comprende al hecho ocurrido e identificado sobre el estado de un sistema, servicio o red que indique un desvío de la política de seguridad establecida, una falla de las medidas de seguridad implementadas o una situación desconocida previamente que pueda ser relevante a la seguridad.

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).

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.

Incidente de seguridad en Canales Electrónicos. Se conforma por el evento o serie de eventos de seguridad, operativos y tecnológicos interrelacionados que generen una exposición no deseada o esperada de las credenciales, transacciones, datos de los clientes y el servicio bancario asociado y que posean una probabilidad significativa de comprometer las operaciones y amenazar la seguridad informática.

Infraestructura de redes. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento y transporte de voz y datos que interconectan e integran los recursos de la infraestructura de tecnología y sistemas.

Infraestructura de seguridad. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento y control de la plataforma tecnológica asociada a la seguridad de los Canales Electrónicos.

Infraestructura de tecnología y sistemas. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento, procesamiento y control de los servicios de tecnología informática asociada a los Canales Electrónicos.

Journal o Tira de auditoría. Comprende a los mecanismos físicos y/o lógicos dispuestos para el 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.

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.

Operadores. Se utiliza el término en forma indistinta para indicar a las empresas prestadoras de servicios financieros dentro de los indicados en esta sección, que cuenten con un acuerdo de servicio con las entidades financieras o actúen en su nombre o cuyas operaciones afecten las cuentas de crédito y/o depósito de sus clientes.

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 con acuerdo de las entidades financieras y operadores de transacciones financieras del Sistema Financiero Nacional

Punto de compromiso. Comprende al individuo, empresa o comercio adquirente de POS en el que se detecta un patrón similar de operaciones sospechosas o fraudulentas con TD/TC.

Puntos de venta (POS). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio al consumidor financiero, que se basan en la utilización de distintos medios de pago electrónico (Tarjetas de Débito/Crédito) para el pago de servicios u operaciones financieras que generen un débito o un crédito en las cuentas bancarias que el cliente posee con el emisor y que confirman tales operaciones mediante la comunicación local o remota con un centro de procesamiento de la entidad emisora o tercero interesado con acuerdo previo del emisor, mediante redes públicas de comunicación aptas y aprobadas por autoridad competente para la transmisión de datos bajo administración de un operador público o privado.

Redes privadas y públicas. Infraestructura de comunicaciones se considera privada cuando es administrada por una entidad financiera o un tercero en su nombre y accesible de forma exclusiva y única para la infraestructura de tecnología y sistemas de la entidad financiera. Se considera pública cuando la infraestructura de comunicaciones es administrada por un operador independiente y accesible mediante suscripción previa a múltiples empresas o individuos.

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

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. Se entenderá compuestos 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 por la persona/comercio y la composición del mensaje correspondiente), ***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.

Tarjetas de Débito/Crédito (TD/TC). Comprende a elementos asociados a las credenciales de acceso a algunos Canales Electrónicos, habitualmente basados en piezas plásticas cuyas inscripciones y características físicas las hacen aptas para su presentación y lectura en dispositivos de autenticación y autorización de los mismos. En la presente norma se mencionan en dos modalidades habituales de uso, como medios primarios de transacciones comerciales de crédito/débito o como medios primarios de acceso a operaciones financieras por ATM ("Automated Teller Machine").

Telefonía fija. Servicios de comunicación ofrecidos por empresas de telecomunicaciones que utilizan los espectros de telefonía fija o terrestre autorizados a nivel nacional, y que incluyen los servicios de enlace e intercambio de voz y datos. Requiere una suscripción personal o comercial con locación del servicio en domicilio específico.

Telefonía móvil. Servicios de comunicación ofrecidos por empresas de telecomunicaciones que utilizan los espectros de telefonía móvil autorizados a nivel nacional, y que incluyen los servicios de enlace e intercambio de voz y datos. Requiere suscripción personal o comercial pero es independiente de la locación del suscriptor.

Terminales de autoservicio (TAS). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio al cliente bancario, que se basan en la utilización de los dispositivos conocidos como Terminales de Autoservicio u otros de similar naturaleza, enlazados a la red institucional de la entidad responsable, ya sea por conexión directa o indirecta (sucursal, proveedor) a un centro de procesamiento y que permitan por lo menos el depósito y transferencia de fondos y excluyan la extracción de efectivo sin intervención de un operador humano.

Transacciones de Bajo Valor. Transacciones financieras por medio de Canales Electrónicos habilitados hasta el máximo establecido en la Comunicación "A" 5982 y sus modificatorias.

6.7. Tablas de requisitos técnico-operativos.

6.7.1. Tabla de requisitos de Concientización y Capacitación.

Tabla de requisitos de Concientización y Capacitación		
Código de requisito	**Descripción de requisito**	**Alcance**
RCC001	Los contenidos del programa de CC deben formularse y mantenerse actualizados en base a un análisis de las vulnerabilidades y los resultados de la Gestión de Incidentes, e incluir, pero no limitarse a incidentes: reportados, detectados y conocidos.	
RCC002	Los contenidos del programa de CC deben incluir: técnicas de detección y prevención de apropiación de datos personales y de las credenciales mediante ataques de tipo "ingeniería social", "phishing", "vishing" y otros de similares características.	
RCC003	Los contenidos del programa de CC deben incluir: técnicas de detección y prevención del "skimming" y apropiación de datos de las credenciales mediante técnicas de intervención física.	
RCC004	Los contenidos del programa de CC deben incluir: técnicas de detección de situaciones sospechosas en el recinto o entorno de acceso al CE.	
RCC005	Mantener informado al personal interno, personal responsable por la gestión del CE, personal de terceros involucrado en las tareas operativas y clientes sobre las vías de comunicación para la recepción de denuncias o problemas en el circuito asociado al escenario descripto.	
RCC006	Respecto de la audiencia del programa de CC, deben aplicarse los siguientes criterios: a. Características y segmentación de la audiencia, de acuerdo con el nivel de intervención en el proceso y naturaleza de la función o rol que ocupa cada participante. b. Deben encontrarse alcanzados todos los participantes necesarios en el flujo completo de la actividad indicada en el escenario. c. Orientado pero no limitado a: personal interno, personal responsable por la gestión del CE, proveedores y clientes.	
RCC007	Con una periodicidad mínima anual, debe efectuarse un análisis del Programa de CC ejecutado que mida la evolución de los incidentes, respecto de las actividades de CC realizadas incluyendo como mínimo: a. Un reporte de la cantidad y segmentación de destinatarios y contenidos del programa de CC. b. Una comparación entre los contenidos cubiertos por el programa de CC y la cantidad y tipo de incidentes de seguridad reportados/detectados/conocidos.	
RCC008	Los contenidos del programa de CC deben incluir: medidas y técnicas para la protección de la privacidad de las credenciales.	
RCC009	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre el uso seguro de los dispositivos propios del usuario y los dispositivos provistos por la entidad/operador.	
RCC010	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre las prácticas de seguridad en la plataforma de soporte de CE.	
RCC011	Los contenidos del programa de CC deben incluir: acciones específicas del usuario para la configuración de los dispositivos propios para comunicación con el CE (teléfonos, computadores personales, tabletas electrónicas, entre otros). Incluye pero no se limita a las características diferenciadas por dispositivo para el almacenamiento de datos, reposo/bloqueo automático, eliminación de información antes del descarte o reemplazo del dispositivo, actualización de sistemas operativos y piezas de software provistas por la entidad para uso del CE.	
RCC012	Los contenidos del programa de CC deben incluir técnicas específicas para el desarrollo/adquisición/fabricación, implementación, homologación y prueba de características de seguridad de los dispositivos y piezas de software provisto por la entidad/operador, asegurando que el personal involucrado interno/externo se encuentra debidamente capacitado para disminuir las fallas de implementación de las características de seguridad.	

Tabla de requisitos de Concientización y Capacitación (continuación)

Código de requisito	Descripción de requisito	Alcance
RCC013	Las entidades/operadores deben contar con un mecanismo de comunicación de los contenidos de su programa de concientización y capacitación que asegure: a. Que los destinatarios se encuentran continuamente informados. b. Que los destinatarios pueden efectuar consultas y evacuar dudas.	
RCC014	En la selección/cambio, por parte del cliente, de los valores de los elementos de autenticación basados en el factor "algo que sabe", la entidad/operador deben recomendar al titular que los valores no se compongan al menos de: a. Una secuencia de número asociado a un dato personal público. b. Serie de caracteres o números iguales. c. Incremento o decremento de número consecutivo. d. Fechas de significación histórica.	

6.7.2. Tabla de requisitos de Control de Acceso.

Tabla de requisitos de Control de Acceso		
Código de requisito	**Descripción de requisito**	**Alcance**
RCA001	Los procesos de distribución de elementos de identificación y autenticación basados en el factor "algo que sabe" deben ser siempre separados de la distribución de los elementos basados en el factor "algo que tiene".	
RCA002	La renovación de factores de identificación y autenticación basados en "algo que sabe" debe permitir la autogestión del cliente bancario o la mínima intervención de un operador durante el proceso, asegurando que solamente el cliente conocerá los valores asignados.	
RCA003	Los elementos de autenticación basados en el factor "algo que sabe" no deben ser conocidos antes ni durante su generación y uso por los funcionarios, empleados, representantes o terceros vinculados con las actividades correspondientes al escenario.	
RCA004	El almacenamiento de valores correspondientes a los factores de autenticación de los clientes bancarios, sólo será permitido cuando estos se encuentren protegidos mediante técnicas que impidan su conocimiento a otros diferentes del cliente y sólo con propósitos de verificación automática de las credenciales presentadas por el cliente para acceder y/o confirmar operaciones en el CE.	
RCA005	Las habilitaciones y rehabilitaciones de los elementos de identificación y autenticación basados en el factor "algo que tiene" deben ser efectuadas mediante un proceso que garantice la identificación positiva del titular (RCA040). Asimismo, estos elementos, sólo podrán estar vinculados durante su uso a una única persona de forma individual e intransferible.	
RCA006	En los dispositivos provistos por la entidad/operador que utilicen teclados físicos (PIN PAD) o teclados virtuales (imagen en pantalla) para el ingreso del factor basado en algo que sabe, el valor ingresado debe ser encriptado inmediatamente después de su ingreso mediante un algoritmo no menor a: a. 3DES para dispositivos que permitan transacciones establecidas con criticidad de nivel 1 en los escenarios del punto 6.5. b. DES para dispositivos que permitan transacciones establecidas con criticidad de nivel distinto a 1 en los escenarios del punto 6.5.	A partir del 01/03/2013, es aplicable a nuevas adquisiciones/desarrollos, reemplazos o actualizaciones de dispositivos/aplicaciones provistos por la entidad/operador.
RCA007	Los sistemas de acceso y verificación de credenciales de los CE contemplados en el escenario descripto, deben garantizar la no reutilización del último valor generado de los elementos de autenticación basados en el factor "algo que sabe" .	
RCA008	La caducidad de los elementos de autenticación basados en "algo que sabe", debe establecerse según el análisis de riesgo de cada entidad o al vencimiento del factor basado en "algo que tiene" asociado al canal, cuando aplique. No obstante, las entidades financieras deben implementar los mecanismos necesarios para que los clientes bancarios puedan voluntariamente realizar el cambio aún antes de ese plazo, así como prevenir su presentación luego de vencido el plazo que determina la validez de los mismos.	
RCA009	Los elementos de autenticación basados en el factor "algo que tiene", siempre que empleen mecanismos de autenticación dinámica (Token, tarjeta de coordenadas, entre otros), deben poseer al menos dos de las siguientes características: a. Mecanismos que impidan su duplicación o alteración (Anti tampering). b. Control de relación unívoca entre cliente/cuenta y dispositivo. c. Identificación única de fabricación. d. Recambio bianual.	
RCA010	Las entidades/operadores, deben aplicar técnicas de protección, según su análisis de riesgo que minimicen la exposición de los factores de identificación y autenticación basados en "algo que tiene", cuando los mismos sean presentados ante dispositivos o medios que revelen a terceros datos confidenciales o códigos de seguridad de las credenciales, en operatorias no presenciales (Internet, WebPos, Venta Telefónica, dispositivos desatendidos), considerando pero no limitándose a las siguientes técnicas: a. Uso de esquemas de verificación complementaria por vías seguras (segundo factor, secretos compartidos, técnicas consideradas en el requisito RCA040). b. Valores aleatorios de identificación de TD/TC (PAN o CVC/CVV variable).	

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA011	Debe limitarse la exposición de los datos identificatorios de las credenciales a aquellos usuarios autorizados por la entidad/operador que por necesidades de uso/conocimiento se encuentren calificados para el acceso a esta información.	
RCA012	En la etapa de inicio de sesión/presentación de credenciales, las entidades/operadores, deben ejecutar acciones específicas para proteger la fortaleza de los factores de identificación y autenticación empleando optativamente: a. Dos factores de autenticación de distinto tipo (autenticación fuerte), en alguna de las combinaciones: "algo que tiene" y "algo que sabe", "algo que sabe" y "algo que es" o,"algo que tiene" y "algo que es". b. Dos factores de autenticación del mismo tipo (autenticación simple), dónde uno de ellos identifique de forma unívoca al usuario.	
RCA013	En caso de falla o indisponibilidad total o parcial de los mecanismos de seguridad (Control de Acceso, Monitoreo, Integridad y Registro) en el dispositivo provisto por la entidad/operador, debe mantenerse inhabilitado totalmente el mismo, informando y previniendo al usuario para que evite la presentación de credenciales y la recepción o entrega de valores.	
RCA014	Los elementos de autenticación basados en el factor "algo que sabe", utilizados en el CE, deben poseer una longitud no inferior a 8 caracteres para BI, 6 caracteres para BM y 4 caracteres para BT.	
RCA015	Los elementos de autenticación basados en el factor "algo que sabe" y sean estrictamente "numéricos" deben: a. Limitarse a elementos del tipo PIN ("Personal Identification Number"). b. Poseer una longitud mínima de 4 dígitos.	
RCA016	Durante todo el ciclo de las tareas asociadas al escenario, los datos y credenciales de un cliente no deben estar en posesión completa de una misma persona o grupo de personas o ser asociados a los datos del cliente salvo por los clientes mismos.	
RCA017	Los elementos de autenticación basados en el factor "algo que sabe" durante sus procesos de generación, uso y transporte deben encontrarse protegidos por medio de alguna de las siguientes técnicas: a. Encripción no menor a 3DES. b. Digesto irreversible o funciones de "hashing". En BT, cuando no se utilice alguna de las técnicas descriptas, se debe garantizar que el mecanismo de autenticación del factor sea distinto al empleado para otros CE de un mismo cliente y entidad financiera.	A partir del 01/03/2013 es aplicable a nuevas adquisiciones/desarrollos, reemplazos o actualizaciones de dispositivos/aplicaciones provistos por la entidad/operador.
RCA018	Los elementos de autenticación basados en el factor "algo que sabe" deben limitar su exposición durante el ingreso o reproducción, en los procesos de generación, renovación y uso, considerando, pero no restringiéndose a la implantación alternativa de: a. Máscaras visuales en la pantalla de dispositivos provistos por la entidad/operador. b. Teclados virtuales en aplicaciones provistas por la entidad/operador. c. Paneles protectores de visualización en los dispositivos provistos por la entidad/operador (ejemplo: PCI PIN - Security Requirement 2.0).	
RCA019	Los procesos de generación de los elementos de identificación y autenticación basados en el factor "algo que tiene" deben realizarse en un esquema de separación de funciones tal, que impida que se combinen con la generación de los elementos de identificación y autenticación basados en el factor "algo que sabe". Ejemplos: embozado de tarjetas y generación de PIN; la instancia de sincronización de un token está diferenciada de su distribución.	
RCA020	Los elementos de identificación y autenticación basados en TD/TC deben contar al menos con las siguientes características: a. Nombre y apellido del cliente bancario. b. Número interno de inscripción (número de tarjeta). c. Firma hológrafa o manuscrita. d. Fecha de vigencia. e. Fecha de vencimiento. f. Número de atención de denuncias.	A partir del 01/03/2013 y sólo para renovaciones y nuevas TD/TC.

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA021	Los procesos de distribución de elementos de identificación y autenticación, basados en el factor "algo que tiene" deben garantizar la identificación positiva del titular antes de su entrega.	
RCA022	Los elementos de identificación y autenticación basados en el factor "algo que tiene", luego de su retención, deben tener una vigencia no mayor a 30 días hábiles para su descarte o desvinculación del cliente y sus cuentas en forma posterior al tiempo determinado en caso de no ser devueltos al cliente.	
RCA023	Los elementos de autenticación basados en el factor "algo que sabe" y "algo que es" deben bloquear el acceso al CE luego de no más de cinco intentos fallidos consecutivos de inicio de sesión, informar al usuario mediante el esquema implementado de alertas tempranas (RCA041) y aplicar un mecanismo de autenticación positiva para el desbloqueo dentro de los considerados en el requisito RCA040. Luego de un tiempo no mayor a 30 minutos desde el último intento fallido registrado, salvo casos de bloqueo, podrá reiniciarse el registro de intentos fallidos.	
RCA024	En caso de falla o indisponibilidad parcial o total de los mecanismos de seguridad (Control de Acceso, Monitoreo, Integridad y Registro) en el servicio provisto por y desde la entidad/operador, debe mantenerse inhabilitado totalmente el servicio, informando y advirtiendo al usuario para que evite la presentación de credenciales desde un dispositivo propio.	
RCA025	En los dispositivos provistos por la entidad/operador que acepten el ingreso (mecanismo de tracción) de TD/TC, y que por falla mecánica u olvido del usuario retuvieran una TD/TC en el dispositivo, la entidad/operador debe proceder a la devolución al titular de la TD/TC o en caso de no hacerse efectiva, a su destrucción en un tiempo no mayor a 10 días hábiles posteriores a su extracción en los procesos de balanceo o mantenimiento del dispositivo.	
RCA026	En todos los casos de factores de autenticación basados en "algo que sabe" que hayan sido generados por la entidad/operador, se deben implementar mecanismos para asegurar que el cliente bancario modifique los valores generados en su primera presentación ante el CE. Dicho cambio, puede efectuarse mediante un CE distinto del considerado en el escenario, siempre que utilice autenticación fuerte.	
RCA027	En todos los casos de factores de identificación de usuarios generados por la entidad/operador se debe ofrecer al usuario la posibilidad de modificar dicho valor a uno elegido por el usuario.	
RCA028	Los elementos de autenticación basados en el factor "algo que sabe", utilizados para el ingreso al CE, deben poseer una composición alfanumérica y una complejidad tal, que incluya al menos la combinación de tres de los siguientes atributos: a. Caracteres especiales. b. Letras mayúsculas. c. Letras minúsculas. d. Números. e. No contener más de dos caracteres alfanuméricos iguales y consecutivos. f. Estar compuestas por datos no triviales (se descartan: números de teléfono, nombres propios, entre otros). Solamente en los canales BM y BT podrán establecerse caracteres exclusivamente numéricos, con una complejidad tal que se prevenga la selección de: g. Serie de caracteres del mismo número. h. Incremento o decremento de número consecutivo.	
RCA029	Los elementos de autenticación de las credenciales basadas en el factor "algo que sabe" y empleados en el inicio de sesión del CE, deben prevenir estar asociadas a datos personales públicos del cliente bancario o de la entidad financiera.	
RCA030	La suscripción a un CE debe realizarse para su aprobación desde un medio que utilice identificación positiva de acuerdo con las técnicas descriptas en el requisito RCA040.	
RCA031	La generación y renovación del PIN asociado a una TD/TC basada en banda magnética según el RCA044 punto a, debe garantizar un valor diferente entre los canales ATM y POS, siempre que se utilice un PIN asociado a una misma TD/TC.	

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA032	La entidad/operador debe ejecutar las siguientes acciones para la protección de las transacciones involucradas en el escenario: a. En el caso de aplicar en la etapa de inicio de sesión/presentación de credenciales, alguna de las técnicas descriptas en el requisito RCA012 punto a. y antes de la confirmación de una transacción de banca individual o grupo interrelacionado de transacciones de banca comercial, debe aplicar técnicas de autenticación complementarias para revalidar la identidad del usuario autorizado, entre las que se incluyen pero no se limitan: secretos compartidos, mecanismos de autenticación simple, rellamada o uso de canal alternativo. b. En el caso de aplicar en la etapa de inicio de sesión/presentación de credenciales, la técnica descripta en el requisito RCA012 punto b. y antes de la confirmación de una transacción de banca individual o grupo interrelacionado de transacciones de banca comercial, debe aplicar alguna de las técnicas descriptas en el requisito RCA012 punto a. para revalidar la identidad del usuario autorizado entre las que se incluyen pero no se limitan: usb tokens, token con generación de contraseña o tarjetas de coordenadas. c. Posterior a la confirmación de la transacción y sólo cuando se superen patrones predeterminados en sus sistemas de monitoreo transaccional, debe aplicar al menos una de las técnicas descriptas en el requisito RCA040. Para el canal ATM, cuando se opere mediante uso de tarjeta con circuito integrado (CHIP) bajo estándar EMV y siempre que se satisfaga el cumplimiento del requisito RCA012 punto a, no será exigible el cumplimiento del punto a del requisito RCA032.	
RCA033	La información referida a mecanismos implementados por una entidad/operador para la seguridad del CE y que sea pieza esencial en la protección del mismo, debe conservarse protegido ante la exposición de su contenido a personas no autorizadas.	
RCA034	Los procesos de implementación, prueba y homologación de dispositivos provistos por la entidad/operador y/o aplicaciones específicas para dispositivos no provistos por la entidad/operador para el uso del CE, cuando lo requieran, sólo podrán utilizar credenciales bajo administración de la entidad/operador, no relacionadas con clientes bancarios y no habilitadas para entornos productivos.	
RCA035	Las piezas de software provistos por la entidad/operador para el uso del CE por medio de un dispositivo propio del cliente, no podrán comprometer la privacidad de estos ni de los datos del cliente contenidos en los mismos aun cuando medie autorización del cliente.	
RCA036	Los dispositivos provistos por la entidad/operador deben contar con características físicas que reduzcan la copia, obstrucción, visualización de terceros o retención ilegal de credenciales y valores monetarios, considerando pero no limitándose a la aplicación alternativa de: a. Detectores de objetos adosados a dispositivos provistos por la entidad/operador. b. Mecanismos de información explícita al usuario de las características del dispositivo provisto por la entidad/operador. c. Componentes anti-skimming en el ingreso de credenciales. d. Mecanismos de detección de apertura, violación o alteración de las condiciones físicas del dispositivo ("tampering detection").	
RCA037	Deben estar descriptos los grupos, roles y responsabilidades para la administración lógica de los componentes de la red de servicios de cada CE.	
RCA038	Los elementos de identificación/autenticación basados en Tarjetas de Débito/Crédito, deben contar con las siguientes características de protección complementaria: a. Impresión de datos de la Tarjeta en bajo o sobre relieve u otra técnica que garantice la legibilidad de los datos identificatorios por al menos el tiempo de vigencia inscripto en la Tarjeta. b. Inclusión de hologramas, códigos de seguridad, entre otros. c. La identificación del emisor y de la entidad bancaria interviniente. d. Los medios de almacenamiento de datos en la Tarjeta (banda magnética, chip, entre otros), no deben almacenar datos completos o legibles de los factores de autenticación.	A partir del 01/03/2013 y sólo para renovaciones y nuevas TD/TC.

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA039	En un dispositivo/aplicación asociado a un CE en el que se utilice un mecanismo de autenticación dinámica (token, softtoken, tarjeta de coordenadas, entre otros) y que permita la ejecución de transacciones financieras consideradas en los escenarios con nivel de criticidad 1 de prefijo ETR, los valores generados para componer las "claves dinámicas", deben satisfacer cómo mínimo las siguientes características durante la petición, validación e ingreso de los valores solicitados: a. La clave dinámica debe poseer una estructura no menor a 4 dígitos numéricos aleatorios. b. Los valores de la clave dinámica generados en cada petición, deben tener una vigencia máxima de 120 segundos o hasta su autenticación, lo que ocurra primero. No se exigirá la vigencia por tiempo cuando la entidad/operador asegure que en la ejecución de transacciones financieras consideradas en los escenarios de prefijo ETR con nivel de criticidad 1, la sesión de un CE emplea un valor nuevo y diferente generado por el dispositivo de autenticación dinámica, tanto en la etapa de "inicio de sesión/presentación" como en la de "confirmación" durante una misma sesión. c. Los valores de la clave dinámica generados en cada petición, no deben ser conocidos antes de su generación y durante el proceso de ingreso y validación de los datos por otros individuos distintos del cliente bancario. d. Debe asegurarse una validación del valor generado que garantice su autenticidad estableciendo una correspondencia efectiva del valor generado en el dispositivo/aplicación con el resto de las credenciales del usuario que forman parte del proceso de autenticación. Por ejemplo mediante una sincronización temporal con los sistemas de autenticación del CE, o por comparación univoca de la semilla de generación. e. Las claves dinámicas tienen validez por única vez en una sola transacción de banca individual y un único grupo de transacciones interrelacionadas en la banca comercial. f. Los procesos de autenticación de la clave dinámica deben ocurrir en línea.	
RCA040	La identificación positiva incluye, pero no se restringe a la utilización combinada o no de las siguientes técnicas: a. Cuestionarios predefinidos con presentación aleatoria, con validación automática del sistema. b. Presentación de documentos de identidad emitidos por autoridad nacional que permitan la comparación y convalidación efectiva de las características del portador. c. Firmas holográficas comparables con registro electrónico. d. Identificación ante canal electrónico alternativo con doble factor de autenticación.	
RCA041	Las entidades/operadores deben poner a disposición de sus clientes la siguiente información, estableciendo mecanismos efectivos de alerta en un tiempo no mayor a 24 horas posteriores a la transacción/sesión y de acuerdo a las características de cada CE, sin perjuicio de incluir información adicional acorde con aquella generada por sus sistemas de monitoreo transaccional: a. Fecha y hora de la última transacción/sesión confirmada en el CE. b. Aviso de vencimiento de las credenciales con una antelación no menor al tiempo operativo necesario para su cambio/reposición. c. Nombres del usuario de la sesión y del titular de la cuenta accedida. d. Datos de contacto del servicio al cliente para reporte de irregularidades/consultas.	
RCA042	Las entidades/operadores deben asegurar que los enlaces/accesos desde sesiones de los CE a sitios no bancarios y/o servicios de un tercero que permitan el acceso y ejecución de transacciones bancarias consideradas en los escenarios del punto 6.5. con prefijo ETR, garanticen el cumplimiento de los mismos requisitos establecidos para el CE y no compartan datos confidenciales de las credenciales con los sitios y servicios del tercero.	
RCA043	Los elementos de identificación y autenticación basados en el factor "algo que tiene" luego de su generación y que permanezcan sin entrega efectiva a su destinatario por más de 90 días, deben: a. Descartarse o reasignarse a otro cliente bancario, en el caso de elementos de autenticación dinámica (tokens, tarjetas de coordenadas, entre otros). b. Descartarse en el caso de TD/TC.	

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA044	Los elementos de identificación y autenticación basados en el factor "algo que tiene" deben contar con códigos de seguridad renovables, diferentes en cada renovación de TD/TC y aplicarse a las transacciones contempladas en los escenarios del punto 6.5. bajo prefijo ETR, de la siguiente forma: a. En TD/TC basadas en banda magnética, deben contar un código de verificación de la credencial no visible y almacenado en la banda (ejemplo: CVV1/CVC1) y un código de verificación de la transacción visible (ejemplo: CVV2/CVC2/CID) impreso en la TD/TC. Opcionalmente y sólo para transacciones cursadas de forma presencial (dispositivo físico POS) podrá sustituirse la implementación del código de seguridad de transacción visible en la TD/TC con algún factor de autenticación del tipo "algo que sabe" o PIN en los términos del requisito RCA031. b. En TD/TC basadas en el uso de circuito integrado (chip) o una combinación de este con otras técnicas, deben contar con un mecanismo de autenticación dinámica y un cifrado de los datos almacenados en el circuito integrado. Puede complementarse con un algún factor de autenticación del tipo "algo que sabe" o PIN en los términos del requisito RCA031.	
RCA045	Las entidades/operadores deben considerar, según sus análisis de riesgo, un reemplazo periódico de los elementos de identificación y autenticación basados en "algo que tiene, por nuevos elementos renovados en sus códigos de seguridad aplicando, por ejemplo, los siguientes criterios: a. Ante las siguientes situaciones presentadas por el tenedor: 1. Denuncia de robo, pérdida o deterioro. 2. Desconocimiento de transacciones efectuadas. b. Ante el vencimiento inscripto en un TD/TC con una antelación mínima de 20 días, deshabilitando en forma inmediata la emisión anterior o activación del reemplazo, lo que ocurra primero. c. Ante la detección de una de las situaciones consideradas en el requisito RMC009. d. Ante cambios de diseño, formato o técnicas de elaboración que modifiquen los elementos de seguridad de las TD/TC se debe proceder con un plan de reemplazo con ejecución no mayor al plazo restante para la renovación original. e. Ante la detección de fallas de fabricación o pérdida durante la distribución y/o almacenamiento. debe procederse al descarte, reemplazo y renovación de todas las TD/TC involucradas. Asimismo, las entidades deben considerar una migración paulatina de las TD/TC a tecnología de microcircuito integrado favoreciendo la expansión del mercado, la seguridad transaccional, la interoperabilidad y la evolución de los servicios financieros.	
RCA046	Las TD/TC basadas en circuito integrado (CHIP) según lo indicado en el requisito RCA044 y que además cuenten con banda magnética (Sistema Dual), no podrán formalizar transacciones mediante el uso de banda magnética cuando la terminal POS o ATM cuente con lector de CHIP habilitado salvo excepciones que deberán quedar con un registro diferenciado y formar parte de los análisis del punto RMC009.	

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA047	En la utilización de TD/TC basadas en circuito integrado (CHIP) bajo estándar EMV, y según el método de autenticación elegido, las entidades y operadores deben: a. Para TD/TC que utilicen el método de autenticación, basados en la verificación de en un dato estático o firma grabada en el CHIP (SDA -Static Data Authentication por sus siglas en Inglés) las transacciones de los escenarios del punto 6.5. bajo prefijo ETR sólo deberán realizarse en la modalidad "en línea" (ver glosario). Del mismo modo, deberán incorporar un segundo factor de autenticación de acuerdo a lo indicado en el requisito RCA032 cuando las transacciones involucren extracciones, transferencias o pagos de bienes y servicios fuera de los límites del concepto "bajo valor" (ver glosario) b. Para TD/TC que utilicen los métodos de autenticación basados en la generación dinámica de claves de autenticación (DDA/CDA – Dynamic Data Authentication/ Combined Dynamic Data Authenticacion), las transacciones de los escenarios del punto 6.5. bajo prefijo ETR podrán realizarse en las modalidades "en línea" o "fuera de línea". Por otra parte, deberán incorporar un segundo factor de autenticación de acuerdo a lo indicado en el requisito RCA032 cuando las transacciones involucren extracciones, transferencias o pagos de bienes y servicios fuera de los límites del concepto "bajo valor" (ver glosario)	
RCA048	En los componentes lectores provistos o no por la entidad/operador para la lectura del factor "algo que tiene" (TD/TC) vinculados o no a dispositivos móviles o computadores personales, deben satisfacerse los siguientes requerimientos:: a. El valor capturado por el lector, debe ser encriptado desde el lector mediante un algoritmo no menor a 3DES para componentes que permitan transacciones establecidas con criticidad de nivel 1 en los escenarios del punto 6.5. b. El lector debe encontrarse asociado de manera univoca a los siguientes tres elementos: (1) red de procesamiento, dispositivo móvil o computador personal, (2) el servicio provisto por la entidad/operador y el (3) cliente/comercio. c. El lector debe ser homologado por la entidad/operador para la provisión del servicio.	

6.7.3. Tabla de requisitos de Integridad y Registro.

Tabla de requisitos de Integridad y Registro		
Código de requisito	**Descripción de requisito**	**Alcance**
RIR001	Los datos de autenticación de las credenciales no deben ser almacenados en el dispositivo provisto por la entidad/operador ni conservados en el registro de actividad del mismo (Journal).	
RIR002	El registro de las actividades en los sistemas aplicativos y/o dispositivos provistos por la entidad/operador, debe garantizar para cada evento al menos: a. Identificación. b. Descripción. c. Fecha y hora completa. d. Identificación de origen. e. Usuario actor.	
RIR003	Los registros colectados por los sistemas aplicativos y/o dispositivos provistos por la entidad/operador deben asegurar la trazabilidad de las acciones realizadas en la totalidad de las actividades, identificando quién (persona/dispositivo/cuenta/oriogen/destino), qué (actividad/función/transacción), dónde (CE, ubicación), cuándo (tiempo) y cómo (patrón/relación de eventos).	
RIR004	Los registros de los sistemas aplicativos y/o dispositivos provistos por la entidad/operador deben contemplar al menos los siguientes eventos: a. Solicitudes y respuestas a acciones transaccionales y de mantenimiento de las aplicaciones. b. Errores y fallas de la aplicación o el dispositivo. c. Intentos exitosos y fallidos de autenticación. d. Gestión de credenciales (alta, eliminación, modificación y asignación de privilegios). e. Gestión de bases de datos/repositorios (creación, eliminación, modificación y consultas). f. Acciones operativas y de mantenimiento (inicio y cierre de los sistemas, fallas y cambios en la configuración).	
RIR005	Los registros de las actividades de cada CE asociado al escenario deben contar desde el momento de su generación, con mecanismos que permitan verificar que cada registro sea único, responda a una secuencia predeterminada y se mantenga inalterable durante su almacenamiento, transporte y recuperación.	
RIR006	Los registros de las actividades de los dispositivos/aplicaciones provistos por la entidad/operador y de las operaciones transaccionales, deben ser almacenados y custodiados mediante alguno de los siguientes regímenes de almacenamiento: a. En el caso de registros digitalizados (Electronic Journal) deben ser enviados en tiempo real o permanecer almacenados por menos de 24 horas en el dispositivo provisto por la entidad/operador que los generó, cuando aplique, debiendo ser trasladados a ese término a una infraestructura de almacenamiento y custodia. b. En el caso de registros impresos (Tira Journal) deben ser enviados en forma inmediata posterior a cada evento de balanceo y carga del dispositivo provisto por la entidad/operador.	
RIR007	Los registros históricos de las actividades y de las operaciones transaccionales deben conservarse por un término no menor a 6 años. Los soportes de almacenamiento del archivo histórico no deben ser recuperables luego de su descarte.	
RIR008	Los soportes de almacenamiento de los registros de las actividades y de operaciones transaccionales en el dispositivo provisto por la entidad/operador no deben ser recuperables luego de los siguientes situaciones: a. 15 días posteriores al traslado confirmado a la infraestructura de custodia y recuperación. b. El descarte del soporte de almacenamiento en el dispositivo.	
RIR009	Los registros de las actividades de los dispositivos/aplicaciones provistos por la entidad/operador y de las operaciones transaccionales, deben contar con mecanismos de protección que aseguren que sólo podrán ser accedidos por aquellos que corresponda según la necesidad de uso/conocimiento.	

Tabla de requisitos de Integridad y Registro (continuación)

Código de requisito	Descripción de requisito	Alcance
RIR010	Los dispositivos y/o piezas de software provistas por la entidad/operador para el uso del CE, deben asegurar que satisfacen un ciclo de vida y de desarrollo de sistemas, basado en las siguientes etapas conceptuales: a. Análisis de requerimientos. b. Adquisición/fabricación/desarrollo. c. Prueba y homologación. d. Implementación. e. Operación y mantenimiento. f. Descarte y reemplazo. Asimismo, este ciclo, debe proveer los elementos de seguridad relacionados con, pero no limitados a: g. Requisitos funcionales de seguridad. h. Tipos y características de validación de los datos de entrada. i. Granularidad de las funciones y los registros. j. Niveles de acceso. k. Control de Cambios. l. Actualización y Parches.	
RIR011	Los procesos de homologación de dispositivos y/o piezas de software provistos por la entidad/operador para interactuar con el CE, deben garantizar la verificación de todos los aspectos de diseño, funcionalidad, interoperabilidad y características de seguridad definidos en las etapas de adquisición/fabricación/desarrollo e implementación.	
RIR012	Los procesos de homologación e implementación de piezas de software del CE en dispositivos del cliente bancario, deben realizarse utilizando una verificación formal antes de su habilitación. Asimismo, deben utilizarse métodos de instalación que prevengan la exposición de datos personales, financieros o de las credenciales del cliente.	
RIR013	Deben efectuarse los siguientes controles de integridad de los datos transmitidos: a. Identificación del receptor y cuenta destino. b. Credenciales y cuenta de origen. c. Identificación y composición del mensaje.	
RIR014	En la transmisión de datos de credenciales y transacciones, todo punto de conexión entre una red privada y una red pública debe contar con un Firewall en cada conexión a Internet y entre cualquier zona desmilitarizada y la zona de la red interna, incluida toda red inalámbrica. Aplica solamente a la infraestructura de la entidad/operador que gestiona el CE con redes basadas en TCP/IP.	
RIR015	Cuando el transporte de datos de credenciales y transacciones se realice mediante el empleo de redes públicas y/o parcialmente privadas en alguno de sus tramos, la entidad/operador debe incluir mecanismos de protección del vínculo y la sesión en los CE, incluyendo pero no limitándose a: a. Uso de protocolos seguros para la transmisión de datos (tales como TLS/SSL/IPSEC/SSH) en redes públicas (tales como 3G, 4G/LTE, GSM, GPRS, WIFI, Internet). b. Uso de métodos de protección del sitio bancario (Certificados digitales basado en infraestructura de clave pública). c. cifrado sólido en redes que utilicen protocolos basados en TCP/IP. Este requisito es únicamente aplicable a los canales TAS, POS y ATM y cuando utilicen redes públicas con protocolos basados en TCP/IP.	
RIR016	En todos los casos, los dispositivos/aplicaciones provistos por la entidad/operador, deben poder generar un comprobante de la transacción efectuada que resulte único y verificable contra los registros de actividad del canal. Incluye pero no se limita a la aplicación alternativa de alguna de las siguientes opciones: a. Papel impreso para dispositivos físicos provistos por la entidad/operador. Emitirse a demanda del cliente en caso que no requiera firma del cliente, obligatoriamente cuando requiera firma del cliente, b. Formato digital para dispositivos propios del cliente, recuperable por al menos 3 meses posteriores a la transacción. Adicionalmente, los datos de identificación de las credenciales del cliente deben limitarse a los estricta y mínimamente necesarios y no deben aparecer de forma completa en el comprobante.	

Tabla de requisitos de Integridad y Registro (continuación)

Código de requisito	Descripción de requisito	Alcance
RIR017	En los procesos de compatibilización de dispositivos y/o implementación de piezas de software en entornos controlados por el usuario, la entidad/operador debe definir e informar al cliente bancario, los requisitos de seguridad aplicables a los dispositivos propios del usuario, realizando las siguientes tareas: a. Informar los criterios de admisibilidad de los dispositivos del usuario, así como las limitaciones de hardware, software, conectividad y entorno para su uso en el CE. b. El CE debe prevenir el acceso a través de un dispositivo que no satisface los criterios de admisibilidad determinados. c. Detectar e informar al usuario las acciones necesarias para mantener habilitado el servicio desde el dispositivo.	
RIR018	Las credenciales basadas en TD/TC que fueran retenidas durante el uso de los dispositivos provistos por la entidad/operador, deben asegurar el cumplimiento de las siguientes acciones operativas: a. Posterior a su retención la entidad/comercio debe informar al emisor antes de transcurridas 24 horas y en el menor tiempo posible de acuerdo con los medios disponibles. b. La entidad/operador emisor debe resolver el incidente en un lapso no mayor a 48 horas. c. En los casos que el material retenido no sea legítimo debe conservarse bajo custodia con los recaudos necesarios para evitar su uso, como material de prueba para posterior investigación.	
RIR019	Las aplicaciones (piezas de software) empleadas para brindar servicios financieros en dispositivos móviles deben garantizar la vinculación única entre la “aplicación”, las credenciales del cliente y el dispositivo móvil, considerando pero no limitándose a las siguientes técnicas combinadas:: a. Asociación de identificador IMEI (International Mobile Station Equipment Identity, por su siglas en inglés) o código único de identificación del dispositivo. b. Semilla para encripción de datos y/o credenciales c. Valor aleatorio que identifica la relación del dispositivo con el servicio financiero. Las aplicaciones para dispositivos móviles deben alojarse en sitios cuyas condiciones de seguridad sean acordes con la política de la entidad financiera y estos ser informados al consumidor de servicios financieros de manera fehaciente.	

6.7.4. Tabla de requisitos de Monitoreo y Control.

Tabla de Requisitos de Monitoreo y Control		
Código de requisito	**Descripción de requisito**	**Alcance**
RMC001	La entidad/operador debe establecer un tiempo máximo de inactividad de la sesión en cada dispositivo/aplicativo provisto al cliente para el uso del CE. Este tiempo debe garantizar que la sesión no permanezca abierta de forma indefinida e incluir pero no limitarse a las siguientes acciones: a. Expiración de la sesión por tiempo establecido para cada canal según análisis de vulnerabilidades documentado. b. Expiración de la sesión en un tiempo no mayor en ningún caso a 30 minutos.	
RMC002	Los dispositivos provistos por la entidad/operador que presenten problemas de comunicación o fallas de funcionamiento total o parcial de los mecanismos de seguridad (Control de Acceso, Integridad y Registro), deben asegurar un monitoreo oportuno basado en alertas y registro de las acciones emprendidas para su inhabilitación/reparación según corresponda.	
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. Este requisito no incluye los dispositivos propios del cliente, ni los elementos de autenticación basados en el factor “algo que tiene” provistos por la entidad/operador.	
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.	
RMC005	Las entidades deben implementar mecanismos de comunicación alternativa con sus clientes con objeto de asegurar vías de verificación variada ante la presencia de alarmas o alertas ocurridas por efecto del monitoreo transaccional implementado.	
RMC006	A partir de los registros colectados por los sistemas aplicativos de la entidad/operador asociados al escenario, se debe realizar una clasificación y determinación de los eventos de seguridad, una definición de los límites y umbrales de compromiso, niveles de comportamiento normal/inesperado y establecer las acciones de acuerdo con cada clasificación y limite determinado.	
RMC007	Los dispositivos provistos por la entidad/operador que interactúen con TD/TC deben contar con mecanismos de alerta en caso de olvido y retención de la TD/TC, con excepción del canal POS.	
RMC008	La entidad financiera debe proveer vías de comunicación para la recepción de consultas/denuncias de los clientes las 24 horas.	

Tabla de requisitos de Monitoreo y Control (continuación)

Código de requisito	Descripción de requisito	Alcance
RMC009	Los sistemas de monitoreo transaccional de las entidades/operadores de TD/TC, deben asegurar la detección, registro y control de situaciones que establezcan un compromiso de datos sensibles que incluya pero no se limite a las siguientes: a. Punto común de compromiso. punto de venta, adquirente, proveedor, entre otros que comprometan transacciones de TD/TC cursadas por el mismo. b. Fuga de información. Pérdida ocurrida en la infraestructura técnica y/o organizacional de la entidad financiera, operador, adquirente, distribuidor y/o proveedores que comprometa información sensible de las TD/TC (números de tarjeta, códigos de seguridad, datos confidenciales del cliente, entre otros) c. Códigos de Seguridad. Compromiso demostrado de los algoritmos de cálculo de los códigos de seguridad de las TD/TC.	
RMC010	Los dispositivos/aplicaciones provistos por la entidad/operador, deben detectar la apertura simultánea de más de una sesión, para un mismo usuario, canal y entidad financiera, ejecutando una de las siguientes acciones: a. Impedir la apertura simultánea de más de una sesión b. Bloquear la operatoria inmediatamente después de la detección, informando al cliente de la irregularidad. El CE ATM podrá exceptuarse de las acciones indicadas en los puntos a y b siempre que se incluyan en los sistemas de monitoreo y control las configuraciones necesarias para detectar y registrar los eventos indicados en el 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.	
RMC012	El proceso de apertura de los dispositivos para ATM y TAS debe garantizar: a. Ser realizada por dos personas, dejando constancia escrita en un acta de su participación y del resultado de la conciliación, balanceo de billetes, conformidad de depósitos, tarjetas retenidas, totales, diferencias si las hubiera, entre otros. b. En los casos de dispositivos neutrales, la documentación de respaldo (planillas o formularios de balanceo, de reposición, de tarjetas retenidas, de conciliación y otras) debe ser firmada, posteriormente, por un funcionario de la entidad financiera, que será la figura responsable para cualquier intervención posterior ante requerimientos de este Banco Central.	
RMC013	Durante los procesos de mantenimiento, configuración, apertura, carga y balanceo de los dispositivos contemplados en el escenario, con excepción del canal POS, se deben satisfacer las siguientes consignas: a. Debe asegurarse una segregación física y lógica de las siguientes funciones: • Administración (instalación, configuración y ajuste de parámetros en el sistema operativo y aplicativo). Debe encontrarse limitada a personal del operador/entidad responsable del servicio. • Operación (ejecución de tareas operativas de consulta, balanceo y reporte). Debe limitarse a responsables de la entidad o tercero contratado por la entidad para los procesos indicados. • Apertura y cierre de dispositivo y tesoro. Debe aplicarse un control dual para el uso y posesión temporal de las llaves físicas y/o lógicas asegurando que en el proceso participan al menos dos personas donde preferentemente una de ellas debe pertenecer a la entidad. b. Debe asegurarse la puesta en práctica de procedimientos internos de la entidad para el control de la documentación de respaldo de las tareas operativas relacionadas.	

6.7.5. Tabla de requisitos de Gestión de Incidentes.

Tabla de requisitos de Gestión de Incidentes		
Código de requisito	**Descripción de requisito**	**Alcance**
RGI001	Debe realizar con una periodicidad mínima anual y con base en el análisis de riesgo de los activos informáticos asociados al escenario, un análisis de los incidentes ocurridos y un reporte que sirva para establecer medidas de protección, contenidos del programa de capacitación y concientización, modificaciones a la registración y control de eventos, y una redefinición de las alertas, límites y umbrales.	
RGI002	La identificación de incidentes debe estar basada al menos en alertas tempranas, estadísticas de tipo/frecuencia/patrón de incidentes y recomendaciones de seguridad informática.	
RGI003	La gestión de incidentes de seguridad puede ejecutarse en forma descentralizada pero debe ser coordinada con personal de la entidad financiera.	
RGI004	No definido.	
RGI005	Los incidentes detectados deben recibir un tratamiento regular con un escalamiento definido formalmente.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS

TEXTO ORDENADO			NORMA DE ORIGEN				Observaciones
Sección	Punto	Párrafo	Com.	Anexo	Punto	Párrafo	
5.	5.4.		"A" 3198		7.1.		Según Com. "A" 4609.
	5.5.		"A" 4609	único	5.5.		
	5.6.		"A" 4609	único	5.6.		
	5.7.		"A" 4609	único	5.7.		
	5.8.		"A" 3198		4.2.1., 6.6. y 6.7.		Según Com. "A" 4609.
	5.9.		"A" 4609	único	5.9.		
	5.10.		"A" 4609	único	5.10.		
	5.11.		"A" 4609	único	5.11.		
	5.12.		"A" 4609	único	5.12.		
6.	6.1.		"A" 4609	único			Según Com. "A" 5374 y 6017.
	6.2.		"A" 3198				Según Com. "A" 4609, 4690, 5374 y 6017.
	6.3.		"A" 4609	único			Según Com. "A" 4690, 5374 y 6017.
	6.4.		"A" 4609	único			Según Com. "A" 4690, 5374 y 6017.
	6.5.		"A" 4609	único			Según Com. "A" 5374 y 6017.
	6.6.		"A" 3198				Según Com. "A" 5374 y 6017.
	6.7.		"A" 4609	único			Según Com. "A" 5374 y 6017.
7.	7.1.		"A" 4609	único	7.1.		
	7.2.		"A" 4609	único	7.2.		
	7.3.		"A" 3198		5.1.		Según Com. "A" 4609.
	7.4.		"A" 3198		5.2. a 5.4.		Según Com. "A" 4609.
	7.5.		"A" 3198		5.5.		Según Com. "A" 4609.
	7.6.		"A" 3198		5.4.		Según Com. "A" 4609.
	7.7.		"A" 3198		5.6.		Según Com. "A" 4609.
8.	8.1.		"A" 3198		9.2.		Según Com. "A" 4609.
	8.2.		"A" 3198		4.2.2.		Según Com. "A" 4609 y 4690 (pto. 6.).
	8.3.		"A" 4609	único	8.3.		
	8.4.		"A" 3198		9.4.		Según Com. "A" 4609.
	8.5.1.		"A" 4609	único	9.1.		
	8.5.2.		"A" 3198		9.1.		Según Com. "A" 4609.