BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" **7370**	**24/09/2021**

A LAS ENTIDADES FINANCIERAS:

Ref.: Circular
RUNOR 1-1695:

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

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

"- Sustituir el requisito técnico-operativo RMC012 –del proceso de monitoreo y control–, establecido en el punto 6.7.4. de 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", por lo siguiente:

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

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

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

b. Que la entidad financiera cancele el crédito preaprobado, asuma la devolución de las sumas involucradas y anule los posibles efectos sobre la situación crediticia de la persona usuaria de servicios financieros afectada, ante la denuncia policial presentada por esta persona usuaria de acuerdo con el modelo de acción "asumido" definido en el requisito RMC004, siempre que la denuncia se presente en un plazo máximo de 90 (noventa) días corridos desde el vencimiento de la primera cuota del crédito.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

En ambos casos, el crédito solicitado podrá acreditarse de manera inmediata en la cuenta del usuario.

La actividad que se realice para el cumplimiento de este requisito debe ser trazable y auditable.”

Por último, les hacemos llegar las hojas que, en reemplazo de las oportunamente provistas, corresponde incorporar en las normas de la referencia. En tal sentido, se recuerda que en la página de esta Institución www.bcra.gob.ar, accediendo a “Sistema Financiero - MARCO LEGAL Y NORMATIVO - Ordenamientos y resúmenes - Textos ordenados de normativa general”, se encontrarán las modificaciones realizadas con textos resaltados en caracteres especiales (tachado y negrita).

Saludamos a Uds. atentamente.

BANCO CENTRAL DE LA REPUBLICA ARGENTINA

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

María D. Bossio
Subgerenta General de Regulación Financiera

ANEXO

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	Para la autorización de un crédito preaprobado la entidad debe verificar fehacientemente la identidad de la persona usuaria de servicios financieros involucrada. Esta verificación debe hacerse mediante técnicas de identificación positiva, de acuerdo con la definición prevista en el glosario y en el requisito técnico operativo específico (RCA040) de estas normas. Asimismo, se deberá constatar previamente a través del resultado del proceso de monitoreo y control, como mínimo, que los puntos de contacto indicados por el usuario de servicios financieros no hayan sido modificados recientemente. Una vez verificada la identidad de la persona usuaria, la entidad deberá comunicarle –a través de algunos de los puntos de contacto disponibles– que el crédito se encuentra aprobado y que, de no mediar objeciones, el monto será acreditado en su cuenta a partir de los 2 (dos) días hábiles siguientes. El citado plazo de acreditación podrá ser reducido en el caso de recibirse la conformidad del usuario de servicios financieros de manera fehaciente. La entidad financiera quedará exceptuada de implementar lo previsto precedentemente, en la medida de que dé cumplimiento a alguna de las siguientes condiciones: a. Que para la autorización de un crédito preaprobado la entidad financiera verifique fehacientemente la identidad de la persona usuaria de servicios financieros involucrada, mediante soluciones biométricas con prueba de vida. b. Que la entidad financiera cancele el crédito preaprobado, asuma la devolución de las sumas involucradas y anule los posibles efectos sobre la situación crediticia de la persona usuaria de servicios financieros afectada, ante la denuncia policial presentada por esta persona usuaria de acuerdo con el modelo de acción “asumido” definido en el requisito RMC004, siempre que la denuncia se presente en un plazo máximo de 90 (noventa) días corridos desde el vencimiento de la primera cuota del crédito. En ambos casos, el crédito solicitado podrá acreditarse de manera inmediata en la cuenta del usuario. La actividad que se realice para el cumplimiento de este requisito debe ser trazable y auditable.	

Tabla de requisitos de Monitoreo y Control (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
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. 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.	

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, 6017, 6209, 6290 y 6684.
	6.4.		"A" 4609	único			Según Com. "A" 4690, 5374 y 6017.
	6.5.		"A" 4609	único			Según Com. "A" 5374, 6017 y 7319.
	6.6.		"A" 3198				Según Com. "A" 5374, 6017 y 6375.
	6.7.		"A" 4609	único			Según Com. "A" 5374, 6017, 6684, 7319, 7325 y 7370.
7.	7.1.		"A" 4609	único	7.1.		Según Com. "A" 6126, 6271 y 6354.
	7.2.		"A" 4609	único	7.2.		Según Com. "A" 6354.
	7.3.		"A" 3198		5.1.		Según Com. "A" 4609 y 6354.
	7.4.		"A" 3198		5.2. a 5.4.		Según Com. "A" 4609 y 6354.
	7.5.		"A" 3198		5.5.		Según Com. "A" 4609, 6354 y 6813.
	7.6.		"A" 3198		5.4.		Según Com. "A" 4609 y 6354.
	7.7.		"A" 3198		5.6.		Según Com. "A" 4609 y 6354.
8.	8.1.		"A" 3198		9.2.		Según Com. "A" 4609.
	8.2.		"A" 3198		4.2.2.		Según Com. "A" 4609 y 4690 (punto 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.