BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" **6375**	**17/11/2017**

A LAS ENTIDADES FINANCIERAS:

Ref.: Circular
CREFI 2 - 103
RUNOR 1 - 1342

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

Nos dirigimos a Uds. para hacerles llegar en anexo las hojas que, en reemplazo de las oportunamente provistas, corresponde incorporar en las normas de la referencia, atento a lo dispuesto por la resolución difundida por la Comunicación "A" 6354.

Asimismo, les señalamos que al último párrafo del punto 2.3. de las normas sobre "Expansión de entidades financieras" y al título del punto 6.6. 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" se les efectuaron adecuaciones formales.

Por último, se recuerda que en la página de esta Institución www.bcra.gob.ar, accediendo a "Sistema Financiero - MARCO LEGAL Y NORMATIVO - Ordenamiento y resúmenes - Textos ordenados de normativa general", se encontrarán las modificaciones realizadas con textos resaltados en caracteres especiales (tachado y negrita).

Saludamos a Uds. atentamente.

BANCO CENTRAL DE LA REPÚBLICA ARGENTINA

Matías A. Gutiérrez Girault
Gerente de Emisión
de Normas

Darío C. Stefanelli
Gerente Principal de Emisión y
Aplicaciones Normativas

ANEXO

-Índice-

2.1. Exigencia de comunicación previa.

Las entidades financieras podrán descentralizar y/o tercerizar actividades que no consistan en la atención de clientes y/o público general (administración, Servicios de Tecnología Informática, archivo, imprenta, etc.) de acuerdo con el siguiente esquema, previa comunicación cursada a la SEFyC con una antelación no inferior a 60 días corridos a la fecha de inicio de esas actividades:

2.1.1. Descentralizar en instalaciones –propias de la entidad, su casa matriz o controlante– y con recursos técnicos y/o humanos propios o de terceros. Esto incluye la descentralización en dependencias o subsidiarias radicadas en el país o en el exterior:

2.1.1.1. de la casa matriz o su controlante, en los casos de sucursales de entidades del exterior;

2.1.1.2. de la controlante –directa o indirecta– del exterior, en los casos de subsidiarias de entidades financieras del exterior;

2.1.1.3. de entidades financieras locales.

2.1.2. Tercerizar en instalaciones de terceros con recursos técnicos y/o humanos propios o de los terceros.

2.2. Condiciones.

2.2.1. Las actividades descentralizadas y/o tercerizadas estarán sujetas a las regulaciones técnicas correspondientes a la naturaleza y tipo de actividades.

2.2.2. En el contrato de tercerización o acuerdo de servicio de descentralización deberá estar expresamente estipulado lo siguiente:

2.2.2.1. La aceptación y el compromiso de cumplimiento de las condiciones a que se refiere el punto 2.2.1., por todas las partes intervinientes.

2.2.2.2. La facultad de la SEFyC para auditar periódicamente el cumplimiento de dichas condiciones.

2.2.3. Para la tercerización de Servicios de Tecnología Informática las entidades deberán implementar un Punto de Acceso Unificado, en los términos indicados en la Sección 7. 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”.

2.2.4. Los agentes en los que se descentralice o tercerice Servicios de Tecnología Informática deberán comprometerse a realizar auditorías internas, como mínimo con una periodicidad anual, respecto de las actividades descentralizadas/tercerizadas, considerando en su alcance lo dispuesto 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” debiendo remitir a la Gerencia de Auditoría Externa de Sistemas los informes de dichas auditorías.

Adicionalmente, deberán remitir los informes de los auditores externos efectuados con motivo de sus revisiones sobre las actividades descentralizadas/tercerizadas.

2.2.5. De acuerdo con lo establecido en el punto 2.2.2.2., las entidades financieras y los terceros que estas contraten deberán comprometerse a permitir que los agentes que designe la SEFyC puedan acceder a las instalaciones donde se presta el servicio descentralizado/tercerizado, cuando ello resulte necesario para cumplir sus funciones de supervisión. Los gastos que se incurran en las revisiones de la actividad descentralizada que se efectúen en el exterior (pasajes, alojamiento, viáticos, traductores, traslados, otros) deberán ser cubiertos en su totalidad por la entidad solicitante a través de la correspondiente transferencia de fondos y/o remisión de los comprobantes de pago pertinentes al BCRA.

2.2.6. Deberán mantenerse en la República Argentina:

2.2.6.1. Los libros y registros contables originales establecidos por las disposiciones legales vigentes, que permitan tanto a la entidad local como a la SEFyC reconstruir y verificar las operaciones y negocios en cualquier momento.

2.2.6.2. El archivo de la información entregada y los documentos firmados por los clientes, que respalden las operaciones activas y pasivas.

2.2.6.3. Los legajos de los deudores, conforme a las normas sobre “Gestión crediticia”.

2.2.6.4. Los documentos y garantías que respalden las financiaciones vigentes otorgadas por la entidad o adquiridas, cuando la entidad compradora tenga a su cargo la administración de la cartera, y la documentación original demostrativa de la propiedad de los restantes activos.

2.2.6.5. Todo resguardo de documentación original, cuando normas legales, reglamentarias y/o disposiciones del BCRA determinen cursos de acción específicos.

2.2.7. Para los casos de actividades descentralizadas en el exterior conforme a lo previsto en el punto 2.1.1., la entidad financiera local, o casa matriz o controlante del exterior, deberá:

2.2.7.1. Obtener del ente supervisor de su país de constitución una certificación escrita en la que conste que:

a) Respecto de la casa matriz o la entidad financiera controlante:

- Se encuentra sujeta a principios, estándares o normas sobre prevención del lavado de activos y del financiamiento del terrorismo internacionalmente aceptados, entre otros los difundidos por el Grupo de Acción Financiera Internacional contra el Lavado de Dinero (FATF-GAFI) y el Comité de Supervisión Bancaria de Basilea.

- El ente supervisor está en conocimiento y no objeta que la sucursal o subsidiaria argentina descentralice actividades en el exterior, y que las tareas correspondientes a dicha descentralización serán parte de su programa normal de supervisión.

b) Respecto de la forma de supervisión:

- Ese organismo de control adhiere a los “Principios básicos para una supervisión bancaria eficaz”, divulgados por el Comité de Supervisión Bancaria de Basilea.

- Aplica supervisión consolidada asumiendo la vigilancia de la liquidez y solvencia así como la evaluación y el control de los riesgos y situaciones patrimoniales considerados en forma consolidada.

2.2.7.2. Establecer un único entorno de control de administración y operación de la tecnología informática y los sistemas de información, que en todo momento permita ejercer el control directo de todas las actividades descentralizadas mediante tecnología implementada en una única locación, cuando la descentralización de actividades se efectúe en una o más locaciones.

2.2.7.3. No estar constituida en países no considerados “cooperadores a los fines de la transparencia fiscal”, en el marco de lo dispuesto por el Decreto N° 589/13, sus normas complementarias y sus modificatorios.

2.2.7.4. Atento al cumplimiento de la Sección 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”, deberán garantizar la continuidad operativa, para todas las actividades descentralizadas y/o información asociada, de las entidades en la República Argentina.

En los casos de entidades financieras locales, sólo deberán observar los puntos 2.2.7.2. y 2.2.7.4. De tratarse de una controlante del exterior que no sea entidad financiera, sólo deberán observarse los puntos 2.2.7.2. a 2.2.7.4.

2.3. Requisitos de la comunicación.

En la comunicación de descentralización de actividades se deberá consignar:

2.3.1. La naturaleza de cada actividad comprendida.

2.3.2. El domicilio donde se desarrollarán las actividades o en el cual se establecerá el entorno de control de administración y operación de la tecnología informática y de los sistemas de información.

2.3.3. La fecha de comienzo de la realización descentralizada de las actividades.

2.3.4. En caso de quedar la realización de las actividades a cargo de un tercero, también deberá adjuntarse copia del contrato de tercerización.

2.3.5. En todos los casos, deberán agregarse las informaciones, compromisos y documentación indicados en los puntos 2.2.1. y 2.2.2., firmados en todos los casos por una persona que acredite facultades suficientes para ello.

La documentación requerida deberá ser enviada a través de la modalidad que la SEFyC establezca en archivo con formato “pdf”, siendo conservados los originales en la entidad financiera a disposición de la SEFyC. El representante legal de la entidad deberá manifestar mediante nota con carácter de declaración jurada que la totalidad de la documentación remitida por medios electrónicos es copia fiel de la documentación que conserva la entidad y se encuentra a disposición de la SEFyC, detallando el lugar donde se encuentra.

2.4. Responsabilidades.

Las entidades financieras que descentralicen actividades no estarán liberadas de sus responsabilidades, presentes o futuras, que les correspondan conforme a las disposiciones legales y reglamentarias y a las normas dictadas por el BCRA.

EXPANSIÓN DE ENTIDADES FINANCIERAS									
TEXTO ORDENADO			NORMA DE ORIGEN						OBSERVACIONES
Secc.	Punto	Párr.	Com.	Anexo	Cap.	Secc.	Punto	Párr.	
	1.7.		"A" 2241		II	5.	5.2. a 5.4.		Según Com. "A" 4382, 4771, 5355, 5983 y 6275.
	1.8.		"A" 2241		II	5.	5.1.		Según Com. "A" 4382, 5983 y 6275.
	1.9.		"A" 5983	único		1.	13.		Según Com. "A" 6275.
2.	2.1.		"A" 3149	I	II	6.	6.1.	1°	Según Com. "A" 5983, 6126 y 6354.
	2.1.1.		"A" 3149	I	II	6.	6.1.1.		Según Com. "A" 6354.
	2.1.2.		"A" 3149	I	II	6.	6.1.2.	1°	Según Com. "A" 5983, 6126 y 6354.
	2.2.1.		"A" 3149	I	II	6.	6.1.	3°	Según Com. "A" 6354.
	2.2.2.		"A" 3149	I	II	6.	6.1.2.	1°	Según Com. "A" 6354.
	2.2.3.		"A" 6354	I					
	2.2.4.		"A" 6354	I					
	2.2.5.		"A" 6354	I					
	2.2.6.		"A" 3149	I	II	6.	6.1.2.3.		Según Com. "A" 6354.
	2.2.7.		"A" 3149	I	II	6.	6.1.2.4.		Según Com. "A" 4949, 5115, 5983, 6126 y 6354.
	2.3.	último	"A" 6354						Según Com. "A" 6375.
	2.3.1.		"A" 3149	I	II	6.	6.1.	2°	
	2.3.2.		"A" 3149	I	II	6.	6.1.	2°	Según Com. "A" 6354.
	2.3.3.		"A" 3149	I	II	6.	6.1.	2°	
	2.3.4.		"A" 3149	I	II	6.	6.1.	2°	
	2.3.5.		"A" 3149	I	II	6.	6.1.2.	último	Según Com. "A" 5983, 6126 y 6354.
	2.4.		"A" 3149	I	II	6.	6.2.		
3.	3.1.		"A" 3149	I	II	6.	6.3.	1°	Según Com. "A" 5983.
	3.2.		"A" 3149	I	II	6.	6.3.	1°	Según Com. "A" 5983.
	3.3.		"A" 3149	I	II	6.	6.3.	2° y último	Según Com. "A" 5983.
4.	4.		"A" 2241		II	9.			Según Com. "A" 6271.
	4.1.		"A" 2241		II	9.	9.2.		Según Com. "A" 5082 y 5983.
	4.1.1.		"A" 2241		II	9.	9.1.1.		Según Com. "A" 5082.
	4.1.2.		"A" 2241		II	9.	9.1.2.		Según Com. "A" 5082.
	4.2.		"A" 5082				9.2.		Según Com. "A" 5983.
	4.3.		"A" 5082				9.3.		
	4.3.1.		"A" 2241		II	9.	9.2. y 9.3.		Según Com. "A" 2512 y 5082.
	4.3.2.		"A" 2241		II	9.	9.3.2.		Según Com. "A" 5082.
	4.3.3.		"A" 2241		II	9.	9.4.		Según Com. "A" 5082.
	4.3.4.		"A" 5082			9.	9.3.4.		
	4.4.		"A" 5082			9.	9.4.		
	4.5.		"A" 5983	único		2.			
	4.5.1.		"A" 5983	único		2.	2.4.1.		
	4.5.2.		"A" 5983	único		2.	2.4.2.		
	4.5.3.		"A" 5983	único		2.	2.4.3.		

Índice

6.6. Glosario.

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.

7.1. Aplicabilidad.

Las entidades financieras podrán contratar –en forma total o parcial– Servicios de Tecnología Informática (STI) provistos por terceros, siempre que se refieran a las actividades que a continuación se contemplan, de acuerdo con los escenarios del punto 7.5. bajo las denominaciones que se indican y cuya definición se encuentra en el glosario previsto en el punto 7.6.:

7.1.1. Infraestructura de Tecnología y Sistemas (SIS).

7.1.2. Procesamiento de Datos (SPD).

7.1.3. Soporte, Prevención y Mantenimiento (SPM).

7.1.4. Comunicaciones (STC).

7.1.5. Almacenamiento y Custodia (SAC).

7.1.6. Desarrollo de Aplicaciones (SDA).

7.1.7. Contingencia y Recuperación (SCR).

7.2. Procesos de seguridad.

De modo referencial y con el objetivo de facilitar la implementación de los requisitos de seguridad determinados, la gestión de seguridad de los STI tercerizados 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 STI tercerizados.

Los procesos 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 satisfaga sus intereses y funcionamiento. Las entidades financieras y los prestadores de los STI tercerizados deben poseer la funcionalidad y propósito descriptos en los procesos de seguridad que a continuación se detallan e informar al Banco Central de la República Argentina (BCRA) la estructura e interrelaciones orgánicas y operativas que en sus organizaciones se corresponda:

7.2.1. Gobierno de la Seguridad de la Información (GS).

Relacionado con la organización de los procesos de administración estratégica y operativa de la seguridad de la información, la estructura funcional y operativa y la determinación de las responsabilidades asociadas.

7.2.2. Concientización y Capacitación (CC).

Relativo a 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 STI tercerizados.

7.2.3. Control de Acceso (CA).

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 STI.

7.2.4. Integridad y Registro (IR).

Destinado a la utilización de técnicas de control de la integridad y registro de los datos y las transacciones, así como el manejo de información sensible de los STI y las técnicas que brinden trazabilidad y permitan su verificación. Incluye, pero no se limita a transacciones, registros de auditoría y esquemas de validación.

7.2.5. Monitoreo y Control (MC).

Relacionado con la recolección, análisis y control de eventos ante fallas, indisponibilidad, intrusiones y otras situaciones que afecten los servicios ofrecidos por los prestadores de STI, y que puedan generar un daño eventual sobre la infraestructura y la información.

7.2.6. Gestión de Incidentes (GI).

Relativo al tratamiento de los eventos y consecuentes incidentes de seguridad en los STI, su detección, evaluación, contención y respuesta, así como las actividades de escalamiento y corrección del entorno técnico y operativo.

7.2.7. Continuidad de las Operaciones (CO).

Relacionado con los recursos y tareas estratégicas y operativas para prevenir, contener y recuperar los procesos críticos del negocio, los servicios financieros y la información crítica ante fallas que afecten la disponibilidad de los STI y la infraestructura informática que los soporta.

7.3. Requisitos generales.

Complementariamente a los requisitos técnico-operativos que se indiquen, las entidades financieras deben satisfacer los siguientes requisitos generales con independencia de la naturaleza, composición y estructura de los servicios que presten por medio de los STI tercerizados.

7.3.1. De la Matriz de Escenarios y la gestión de riesgo operacional de tecnología.

7.3.1.1. Deben encuadrar la operatoria de los STI tercerizados que gestionen dentro de los escenarios comprendidos en la matriz de escenarios contenida en el punto 7.5., implementando como mínimo y según la criticidad que se establezca los requisitos indicados para cada escenario aplicable.

7.3.1.2. Atento a las normas sobre “Lineamientos para la gestión de riesgos en las entidades financieras”, las entidades financieras deben incluir en su análisis de riesgo operacional todos los activos informáticos relacionados con los escenarios aplicables, estableciendo un nivel de criticidad equivalente al indicado por el BCRA para cada escenario o, cuando no esté indicado, por lo establecido en el punto 7.4.2.

7.3.1.3. Lo indicado en el punto 7.3.1.2. debe encontrarse documentado y formar parte de la metodología de gestión de riesgo operacional de la entidad financiera. A su vez, es complementario de los análisis de riesgo periódicos y los mecanismos de seguridad informática implementados para minimizar los riesgos detectados.

7.3.1.4. Los errores de encuadramiento en los escenarios, 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 (SEFyC) un informe de las adecuaciones efectuadas avalado por una verificación de conformidad de su auditoría interna, posterior al vencimiento de plazo indicado. La SEFyC podrá realizar una verificación de lo actuado.

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

7.3.2.1. 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 financieras deben contar con funciones y tareas relacionadas con los siguientes procesos estratégicos de seguridad para sus STI tercerizados:

i) Complementariamente a lo indicado en el punto 7.2.1. (GS), las entidades deben desarrollar, planificar y ejecutar un Programa de Seguridad de la Información con el objetivo de proteger los activos, procesos, recursos técnicos y humanos relacionados con los STI tercerizados bajo su responsabilidad, basado en un análisis de riesgo de actualización periódica mínima anual, integrado a la gestión de riesgo, en su correspondencia con la Matriz de Escenarios y en los requisitos técnico-operativos detallados en el punto 7.7.

ii) Complementariamente a lo indicado en el punto 7.2.2. (CC), 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 STI tercerizados con los que cuentan.

iii) Complementariamente a lo previsto en el punto 7.2.3. (CA), 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 disponibilidad, la reducción de la complejidad de uso y la maximización de la protección de la información del cliente.

iv) Complementariamente a lo indicado en el punto 7.2.4. (IR), las entidades deben garantizar un registro y trazabilidad completa de las actividades de los STI tercerizados en un entorno seguro para su generación, almacenamiento, transporte, custodia y recuperación.

v) Complementariamente a lo previsto en el punto 7.2.5. (MC), las entidades deben contar con recursos técnicos y humanos dispuestos para asegurar un control permanente y continuo de todos sus STI tercerizados y una clasificación de los eventos registrables, así como patrones de búsqueda y correlación.

vi) Complementariamente a lo indicado en el punto 7.2.6. (GI), las entidades deben arbitrar los esfuerzos necesarios para contar en sus organizaciones con recursos técnicos y humanos especializados en la atención, diagnóstico, análisis, contención, resolución, escalamiento e informe de los incidentes de seguridad de todos sus STI tercerizados, de manera formal e integrada.

vii) Complementariamente a lo indicado en el punto 7.2.7. (CO), las entidades deben establecer criterios de continuidad y recuperación para cada uno de los STI tercerizados y contar con los recursos técnicos y humanos así como los planes necesarios para garantizar la continuidad operativa según la demanda de cada servicio, el soporte técnico y logístico, la recuperación de datos y sistemas aplicativos y el procesamiento alternativo en contingencia.

7.3.2.2. Punto de Acceso Unificado. Las entidades deberán implementar un entorno no operativo que permita ejercer el control activo, continuo y permanente de todas las actividades indicadas en el acuerdo de STI tercerizado y los datos, mediante un punto de acceso emplazado en la República Argentina, bajo administración de la entidad, independientemente de las locaciones, cantidad y naturaleza de los servicios provistos y/o que la tercerización ocurra parcial o totalmente con recursos propios, de dependencias, subsidiarias o terceros contratados. El mismo deberá aplicarse de manera no exhaustiva a las siguientes condiciones:

i) Deberá tener el mismo nivel de criticidad asignado al escenario de mayor criticidad en el que se encuentre encuadrado el STI, de acuerdo con lo establecido en los puntos 7.4. y 7.5.

ii) Deberá permitir la verificación de los requisitos dispuestos en los escenarios en los que encuadre cada STI tercerizado.

iii) Deberá proveer los mecanismos de visualización, seguimiento y reporte de información de toda la actividad en curso y pasada, con el nivel de granularidad establecido por los requisitos de cada escenario, así como los reportes de control, análisis, resultados, planes, pruebas, capacitaciones, certificaciones y auditorías practicadas por sí o por terceros a los STI.

7.3.3. De la responsabilidad sobre los STI tercerizados.

7.3.3.1. El Directorio -o autoridad equivalente de la entidad- es el responsable de la gestión de tecnología y seguridad informática de la operatoria de los STI tercerizados, debiendo establecer contratos formales en los que se detallen todos los servicios tercerizados, su funcionamiento y los mecanismos de control previstos.

7.3.3.2. La responsabilidad de las entidades financieras en los servicios y operaciones cursadas por medio de STI tercerizados incluye, pero no se limita, a los medios operativos, físicos y lógicos de acceso e intercambio de información con los usuarios, la infraestructura de procesamiento, transporte y custodia de información operativa y financiera.

7.3.3.3. Las empresas prestadoras de STI tercerizados, que incluyen el procesamiento, transporte, custodia, desarrollo de aplicaciones, continuidad operativa y/o tareas o procesos informáticos de las entidades financieras, incluyendo a los propietarios de licencias o marcas que por acuerdo con las entidades financieras facilitan el uso de sus recursos e infraestructura, deberán cumplir las condiciones establecidas en esta sección y en la Sección 2. de las normas sobre “Expansión de entidades financieras” y en otras regulaciones técnicas complementarias.

7.3.3.4. Las entidades financieras deben establecer e informar al BCRA la estructura orgánica dispuesta y la nómina de responsables de las tareas relacionadas con los Procesos de Seguridad indicados en el punto 7.2. y comunicar cualquier novedad o cambio efectuado a la nómina en un plazo no mayor a 10 días hábiles luego de ocurrido el hecho. Esta información incluye: los procesos, tareas y responsables en empresas prestadoras donde se encuentre tercerizada parte o la totalidad de los STI.

7.3.3.5. De acuerdo con lo establecido en las normas sobre “Expansión de entidades financieras”, las entidades deben contar para la supervisión, control y monitoreo continuo y permanente, de un servicio bajo su administración directa denominado Punto de Acceso Unificado, que deberá satisfacer los requisitos establecidos en los escenarios correspondientes del punto 7.5.

7.3.3.6. Con el objeto de que el BCRA 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 STI tercerizado no contemplado en el punto 7.1. o modalidad operativa diferente de las contempladas en esta sección.

7.4. Escenarios de STI tercerizados.

7.4.1. Guía de uso.

Cada escenario está compuesto por una situación inherente a la protección de los datos gestionados por intermedio de un STI, una determinación de la aplicabilidad del escenario en los STI tercerizados 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.

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 STI tercerizados considerados en la norma y en el escenario en particular. No aplica el mismo escenario descripto a todos los tipos de servicios tercerizados contemplados en el punto 7.1.

7.4.2. Criticidad y cumplimiento.

La criticidad es un ponderador que establece el nivel de importancia relativo de un escenario y sus necesidades regulatorias, considerándose siempre mayor criticidad a los datos personales y financieros del cliente, independientemente del servicio que lo soporta. 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 el punto 7.4.1.

El nivel de obligación de las entidades de cumplir los requisitos técnico-operativos se encuentra determinado por tres elementos: el encuadramiento indicado en el punto 7.3.1.1., la criticidad asignada al escenario 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 contemplado 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 y confiabilidad de los STI, entidades financieras 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 de los STI en el Sistema Nacional de Pagos o Sistema Financiero Nacional. • Interoperabilidad y efectos sobre otros STI tercerizados o no.	Obligatorio. Las entidades financieras y sus prestadores de STI deben satisfacer los requisitos técnico- operativos de cada escenario de acuerdo con la correspondiente Tabla de Requisitos.
2	Moderada exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma limitada la disponibilidad y confiabilidad de los STI, entidades financieras y el sistema financiero en general.		Alineado. Las entidades financieras y sus prestadores de STI 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 correspondiente Tabla de Requisitos.
3	Baja exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma limitada la disponibilidad y confiabilidad de los STI, entidades financieras o el sistema financiero en general.		Esperado. Las entidades financieras y sus prestadores de STI 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 del BCRA. 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.

7.5. Matriz de escenarios.

Matriz de Escenarios					
Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos Mínimos
STI tercerizados en el país o el exterior	ESD001	Datos del cliente. uso/explotación, conservación y transporte, incluyendo transacciones financieras que incluyan datos del cliente.	SPD; SPM; STC; SDA; SAC; SCR.	**1**	RGS001; RGS002; RGS003; RGS004; RGS005; RGS006; RGS007; RCC001; RCC002; RCC005; RCC006; RCC007; RCC008; RCC010; RCC012; RCC013; RCA049; RCA050; RCA051; RCA052; RIR003; RIR010; RIR011; RIR020; RIR021; RIR022; RIR023; RIR024; RMC004; RMC006; RMC014; RMC015; RGI001; RGI002; RGI003; RGI005; RCO001; RCO002; RCO003; RCO004.
	ESD002	Datos contables-financieros: uso/explotación, conservación y transporte, incluyendo o no datos de clientes.	SPD; SPM; STC; SDA; SAC; SCR.	**1**	RGS001; RGS002; RGS003; RGS004; RGS005; RGS006; RGS007; RCC001; RCC002; RCC005; RCC006; RCC007; RCC008; RCC010; RCC012; RCC013; RCA049; RCA050; RCA051; RCA052; RIR003; RIR010; RIR011; RIR020; RIR021; RIR022; RIR023; RIR024; RMC004; RMC006; RMC014; RMC015; RGI001; RGI002; RGI003; RGI005; RCO001; RCO002; RCO003; RCO004.
	ESD003	Datos transaccionales financieros: uso/explotación, conservación y transporte que no incluya datos del cliente.	SPD; SPM; STC; SDA; SAC; SCR.	**2**	RGS001; RGS004; RGS005; RGS007; RCC001; RCC005; RCC006; RCC007; RCC010; RCC012; RCC013; RCA050; RCA051; RCA052; RIR003; RIR010; RIR011; RIR021; RIR022; RIR023; RMC004; RMC006; RMC014; RMC015; RGI001; RGI002; RGI003; RGI005; RCO001; RCO002; RCO003; RCO004.
	ESD004	Datos operativos: uso/explotación, conservación y transporte que no incluya información contable-financiera, del cliente o transaccional financiera.	SIS; SPD; SPM; STC; SDA; SAC; SCR.	**2**	RGS001; RGS004; RGS005; RGS007; RCC001; RCC005; RCC006; RCC007; RCC010; RCC012; RCC013; RCA050; RCA051; RCA052; RIR003; RIR010; RIR011; RIR021; RIR022; RIR023; RIR025; RMC003; RMC006; RMC014; RMC015; RGI001; RGI002; RGI003; RGI005; RCO001; RCO002; RCO003; RCO004.

7.6. Glosario.

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 cuyos resultados esperados sean relevantes para la entidad.

Almacenamiento y Custodia (SAC). Comprende todos los recursos informáticos, operativos y de información dispuestos para el registro, conservación, recupero y explotación de datos integrados a un STI.

Cliente - usuario de servicios financieros - usuario. Los términos “cliente” y “usuario de servicios financieros” son equivalentes y se refieren a la persona humana 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.

Comunicaciones (STC). Abarca a todos los recursos informáticos y operativos dispuestos para la administración, operación, disponibilidad, mantenimiento y transporte de voz, datos, imagen o video que se interconectan e integran a los recursos de la infraestructura de tecnología y sistemas (SIS) de un STI.

Contingencia y Recuperación (SCR). Comprende a todos los recursos informáticos y operativos dispuestos para la administración, operación y mantenimiento de los procesos de continuidad operativa, recuperación de datos, procesamiento alternativo, soporte técnico y logístico en contingencia, de acuerdo con la demanda establecida para cada STI.

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

Datos contables-financieros. Se refiere a toda información referida a saldos, balances y activos de la entidad financiera o de sus clientes no individualizados.

Datos operativos. Comprende toda información referida a la administración, gestión, tareas e instrucciones sobre los recursos técnicos de una entidad financiera y/o tercerizados, incluyendo, pero no limitándose, a los procesos de tecnología y sistemas, excluyendo datos del cliente, datos contables-financieros y datos transaccionales financieros.

Datos transaccionales financieros. Comprende de manera particular a las instrucciones individuales o relacionadas que ordenen movimientos financieros en cuentas bancarias de uno o varios clientes, pasibles de verificación y aprobación antes de su perfeccionamiento o confirmación.

Desarrollo de aplicaciones. Abarca a todos los recursos humanos y de software, metodología, licencias, diseño, conocimiento, mano de obra, prueba y mantenimiento para la programación/adquisición de piezas de software aplicativo o rutinas programadas para el uso/explotación de datos productivos.

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 en los STI.

Evento. Comprende al hecho ocurrido e identificado sobre el estado de un sistema, servicio o red que indique un desvío de la expectativa establecida para un STI, una falla de las medidas de seguridad implementadas o una situación desconocida previamente que pueda ser relevante a la integridad, disponibilidad y/o confidencialidad de la información y los STI en general.

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

Infraestructura de seguridad. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento y control de la seguridad de los STI.

Infraestructura de tecnología y sistemas (SIS). Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, desarrollo, mantenimiento, procesamiento y control de los STI.

Journal o Tira de auditoría. Se refiere a los mecanismos físicos y/o lógicos dispuestos para el registro de la actividad de los STI asociados al acceso e instrucción de operaciones.

Prestadores. Se utiliza el término en forma indistinta para indicar a las empresas prestadoras de STI dentro de los indicados en esta sección, que cuenten con un acuerdo de servicio con las entidades financieras o actúen en su nombre.

Soporte, prevención y mantenimiento (SPM). Comprende todos los recursos humanos, informáticos y operativos dispuestos para brindar soporte, mantenimiento, técnicas de prevención y/o análisis de datos de los STI.

Movimientos financieros. Comprende el registro de movimientos de crédito y/o débito y/o consultas confirmados en cuentas bancarias de un cliente.

Procesamiento de datos (SPD). Comprende todos los recursos humanos, informáticos y operativos dispuestos para la operación, ingreso, transformación y salida de datos mediante el uso de funciones, instrucciones o aplicaciones programadas de manera controlada y repetitiva, integrados a un STI.

Redes privadas. Infraestructura de comunicaciones 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.

Redes públicas. Infraestructura de comunicaciones administrada por un prestador independiente y accesible mediante suscripción previa a múltiples empresas o individuos.

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

Servicios de Tecnología Informática (STI). Comprende a la prestación formal, regular, periódica, delimitada y controlada de recursos de tecnología informática indispensables para brindar alguno o varios de los siguientes servicios: infraestructura informática, procesamiento de datos, operaciones y mantenimiento, comunicaciones, almacenamiento y custodia, desarrollo de aplicaciones y contingencia; siempre que los mismos tengan un impacto directo o indirecto sobre datos del cliente, datos contables-financieros o datos transaccionales.

STI tercerizados. Corresponde a la prestación de servicios de administración y/o gestión operativa informática, mediante acuerdos con terceros, que cuenten con recursos aptos para ofrecer servicios de tecnología informática (STI) que pueden ser prestados parcial o totalmente a una o más organizaciones de manera conjunta o individualizada en el país o en el exterior en conformidad con lo establecido en las normas sobre “Expansión de entidades financieras”.

7.7. Tablas de requisitos técnico-operativos.

7.7.1. De Gobierno de seguridad de la información.

Tabla de requisitos técnico-operativos de Gobierno de Seguridad de la Información		
Código de requisito	**Descripción de requisito**	**Vigencia/Alcance**
RGS001	Las entidades/prestadores deberán establecer y notificar al BCRA el detalle completo, exhaustivo y actualizado de las responsabilidades compartidas y/o exclusivas sobre los roles y funciones para la administración y gestión operativa de seguridad de la información asociadas al STI.	
RGS002	La entidad/prestador deberá establecer roles y funciones para el tratamiento de los datos del cliente, estableciendo las responsabilidades correspondientes según el nivel de participación y tarea que realice. Estas obligaciones deberán estar formalizadas en los acuerdos del STI.	
RGS003	La entidad y el prestador del STI tercerizado deberán cumplir con las leyes y regulaciones nacionales relacionadas con la protección de datos personales (Ley 25.326) cuando el servicio involucra la recolección y uso de datos personales, lo que deberá reflejarse en los acuerdos del STI.	
RGS004	La entidad y prestador deberán establecer y documentar los protocolos de intercambio de información entre los participantes del acuerdo de STI, incluyendo terceros subcontratados, así como las técnicas y medidas operativas (formatos, límites de tiempo, responsables, etc.) que garanticen información útil, oportuna y completa a las partes involucradas y al BCRA.	
RGS005	En el caso de prestador o subcontratistas participantes de un STI que procesen, almacenen o transporten datos o procesos de la entidad en locaciones en el exterior, la entidad, los prestadores y los terceros involucrados deberán proveer los mecanismos necesarios para verificar si las locaciones satisfacen las disposiciones legales, normativas y contractuales establecidas en el acuerdo de STI, incluyendo lo establecido en las normas sobre "Expansión de entidades financieras".	
RGS006	El acuerdo de STI deberá incluir la obligación de no divulgación de datos personales y extender tal obligación a terceros subcontratados.	
RGS007	Las entidades/prestadores deben documentar y asignar la propiedad de todos los activos de información en el STI, determinando el nivel de responsabilidad administrativa y operativa de cada parte en el ciclo de vida de la información.	

7.7.2. De Concientización y Capacitación.

Tabla de requisitos técnico-operativos de Concientización y Capacitación		
Código de requisito	**Descripción de requisito**	**Vigencia/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.	
RCC005	Mantener informado al personal interno, personal responsable por la gestión del STI, 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 STI, proveedores y clientes.	

Tabla de requisitos técnico-operativos de Concientización y Capacitación		
Código de requisito	**Descripción de requisito**	**Vigencia/Alcance**
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.	
RCC010	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre las prácticas de seguridad en la plataforma de soporte de STI.	
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 recursos informáticos del STI, asegurando que el personal involucrado interno/externo se encuentra debidamente capacitado para disminuir las fallas de implementación de las características de seguridad.	
RCC013	Las entidades/prestadores deben contar con un mecanismo de comunicación de los contenidos de su programa de concientización y capacitación del STI que asegure: a. Que los destinatarios se encuentran informados de forma continua. b. Que los destinatarios pueden efectuar consultas y evacuar dudas.	

7.7.3. De Control de Acceso.

Tabla de requisitos técnico-operativos de Control de Acceso		
Código de requisito	**Descripción de requisito**	**Vigencia/Alcance**
RCA049	La entidad y prestador deberán garantizar que los datos personales no sean accedidos/procesados/explotados por ellos o cualquiera de sus proveedores para fines diferentes de los establecidos en los acuerdos formales del STI, ni se realicen sin el formal y expreso consentimiento del responsable primario de los datos.	
RCA050	Las entidades/prestadores deben garantizar el acceso irrestricto a la entidad y al BCRA, a toda documentación e información relativa al procesamiento, operaciones y procedimientos del STI cuando sea requerida.	
RCA051	La entidad debe asegurar que el prestador del STI documente y respalde el nivel de controles implementados para la protección de los servicios provistos, por medio de mediciones independientes, auditorías externas y certificaciones de estándares internacionales.	
RCA052	Las entidades/prestadores deben contar e implementar con una política homogénea de administración de credenciales, basada en la necesidad de uso/conocimiento, la separación de roles incompatibles y la prevención de colusiones, para el acceso a, pero sin limitarse a: • Mecanismos de encripción de datos y canales de comunicación. • Usuarios privilegiados de la plataforma operativa/aplicativa. • Usuarios de emergencia/contingencia. • Usuarios comunes. Asimismo, deberán asegurar un ciclo de vida de las credenciales, cuyos parámetros, reglas, algoritmos, piezas de software involucradas deberán ser actualizadas y debidamente comunicadas a las partes.	

7.7.4. De Integridad y Registro.

Tabla de requisitos técnico-operativos de Integridad y Registro		
Código de requisito	**Descripción de requisito**	**Vigencia/Alcance**
RIR003	Los registros colectados por los servicios provistos por el prestador, deben asegurar la trazabilidad de las acciones realizadas en la totalidad de las actividades, identificando quien (cuenta, origen, destino), qué (actividad, función, transacción), dónde (servicio, ubicación), cuando (tiempo), cómo (patrón, relación de eventos).	
RIR010	Los dispositivos/equipamiento y/o piezas de software dispuestas por la entidad/prestador para el STI, deben asegurar que satisfacen un ciclo de vida y de desarrollo, 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	Las entidades/prestadores deben ejecutar un proceso de homologación de dispositivos/equipamientos y/o piezas de software para interactuar con el STI, garantizando la verificación de todos los aspectos de diseño, funcionalidad, interoperabilidad y características de seguridad definidos en las etapas de adquisición/fabricación/desarrollo e implementación.	
RIR020	Las entidades/prestadores deben contar con mecanismos preventivos y correctivos para la atención de reclamos por el acceso, modificación y eliminación de datos personales, ante requerimientos al amparo de la protección de derechos del cliente.	
RIR021	Las entidades/prestadores deben garantizar y establecer los mecanismos de recupero de los activos de información ante rescisión/terminación y/o interrupción indefinida de los servicios y/o relocalización, respetando las condiciones de seguridad de la información y continuidad de las operaciones.	
RIR022	Los recursos e información que se utilicen en el STI deben estar inventariados con su correspondiente identificación del propietario e indicando los parámetros de eliminación segura y sus parámetros de validación en el ciclo de vida del dato.	
RIR023	Las entidades/prestadores deben establecer un ciclo de vida de los datos de registro de las actividades, según lo establece el requisito RIR003, cumpliendo con los requerimientos legales y las previsiones de seguridad para su almacenamiento, inalterabilidad por el tiempo legal de conservación y su accesibilidad a los responsables del control para soporte de investigaciones forenses en casos de incidentes de seguridad y detección de brechas de seguridad.	
RIR024	Las entidades/prestadores, deben establecer una política de encripción de los datos estén en reposo, tránsito o en ambos estados, incluyendo la asignación de la responsabilidad para los controles definidos en cada estado del dato.	
RIR025	Las entidades/prestadores deben asegurar una separación lógica de los ambientes de procesamiento, almacenamiento, transporte y recuperación de datos de la entidad respecto del prestador, otras entidades y terceros. Asimismo, deben asegurar que los dispositivos/equipamientos y piezas de software que se empleen o accedan a los entornos de la entidad, deben restringirse a los necesarios y homologados según lo indicado en el requisito RIR011.	

7.7.5. De Monitoreo y Control.

Tabla de requisitos técnico-operativos de Monitoreo y Control		
Código de requisito	**Descripción de requisito**	**Vigencia/Alcance**
RMC003	Las entidades/prestadores deben realizar un seguimiento en los STI de los cambios de configuración de seguridad y verificar los niveles de actualización de: sistemas operativos, bases de datos, vínculos de comunicación, herramientas de prevención y detección de códigos maliciosos, equipamientos de seguridad de red, controladores de tráfico y cualquier otra herramienta de seguridad. Deben incluir, pero no limitarse a: a) Seguimiento de privilegio y derechos de acceso; b) Procesos de copia, resguardo y recuperación de información; c) Disponibilidad de los dispositivos/equipamiento; d) Alarmas, alertas y problemas detectados por los sistemas de registro de eventos.	
RMC004	Las entidades/prestadores deben disponer de mecanismos monitoreo transaccional en los STI que operen basados en características del perfil y patrón transaccional del cliente en alguno de los siguientes modelos de acción: a) Preventivo. Detectando, disparando acciones de comunicación con el cliente por vías alternativas 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.	
RMC006	A partir de los registros colectados por los recursos del STI asociados al escenario, las entidades/prestadores deben 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 límite determinados.	
RMC014	Las entidades/prestadores deben determinar, documentar y procedimentar los recursos, dispositivos/equipamientos y piezas de software para monitorear las actividades de los STI.	
RMC015	Las entidades/prestadores deben establecer formalmente y ejecutar periódicamente tareas de prueba y análisis de vulnerabilidades de los recursos asociados al STI en todos sus procesos críticos.	

7.7.6. De Gestión de Incidentes.

Tabla de requisitos técnico-operativos de Gestión de Incidentes		
Código de requisito	**Descripción de requisito**	**Vigencia/Alcance**
RGI001	Las entidades/prestadores deben 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 tercerizada pero debe ser coordinada con personal de la entidad financiera.	
RGI005	Los incidentes detectados deben recibir un tratamiento regular con un escalamiento definido formalmente.	

7.7.7. Tabla de requisitos mínimos de Continuidad Operativa.

Tabla de requisitos técnico-operativos de Continuidad Operativa		
Código de requisito	**Descripción de Requisito**	**Comentarios**
RCO001	Se debe contar con la provisión de los recursos necesarios para la creación, mantenimiento, actualización y prueba de un plan de continuidad del procesamiento de datos. El mismo debe ser operable y funcional, en base a los requerimientos acordados en el STI, propios de la entidad y regulados por el BCRA.	
RCO002	Las entidades/prestadores deben definir, acordar, documentar y poner en ejecución los métodos para determinar el impacto de un evento que interrumpa las actividades de la organización tanto de la entidad, el prestador o terceros subcontratados contemplando, pero no limitándose, a: i) Identificación de recursos críticos, incluyendo usuarios operativos y de control; ii) Identificación de todas las dependencias, incluyendo procesos aplicaciones, pares, y terceros subcontratados; iii) Detección de las amenazas de los recursos críticos; iv) Determinación del impacto de las interrupciones planeadas o no, y su variación en el tiempo; v) Establecimiento de un periodo máximo tolerable de interrupción; vi) Establecimiento de periodos de recuperación parciales y totales; vii) Establecimiento del tiempo máximo tolerable de interrupción para la recuperación de recursos críticos; viii) Estimación de los recursos requeridos para la continuidad y eventual restauración de la operatoria y locaciones alternativas. Debe asimismo, darse participación activa a los responsables primarios de los procesos y recursos críticos, garantizando una cobertura completa de los asociados al STI.	
RCO003	El plan de continuidad de procesamiento de datos debe, considerar, pero no limitarse a la incorporación de los siguientes contenidos: a) Procedimientos operativos manuales, logísticos y automatizados de emergencia según cada proceso/recurso identificado y acción determinada; b) Ubicación/locación, traslado y transporte de responsables, proveedores y servicios de emergencia y recursos físicos y lógicos; c) Procedimientos de recuperación/restauración de los recursos comprometidos.	
RCO004	El plan de continuidad de procesamiento de datos debe ser probado periódicamente, como mínimo una vez al año. Las pruebas deben ser consistentes y coherentes con los criterios del requisito RCO002. Las pruebas también deben garantizar que todos los responsables y participantes de los procesos de continuidad y recuperación se encuentren informados de manera regular, continua y formal.	

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 y 6290.
	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, 6017 y 6375.
	6.7.		"A" 4609	único			Según Com. "A" 5374 y 6017.
7.	7.1.		"A" 4609	único	7.1.		Según Com. "A" 6126, 6271 y 6354.
	7.2.		"A" 4609	único	7.2.		Según Com. 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 y 6354.
	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 (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.