BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" **7724**	**10/03/2023**

A LAS ENTIDADES FINANCIERAS:

Ref.: Circular
RUNOR 1-1785:

Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información.

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

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

3. Establecer que la presente comunicación tendrá vigencia a los 180 días corridos contados desde su difusión."

Saludamos a Uds. atentamente.

BANCO CENTRAL DE LA REPÚBLICA ARGENTINA

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

María D. Bossio
Subgerenta General
de Regulación Financiera

ANEXO

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

B.C.R.A.	TEXTO ORDENADO DE LAS NORMAS SOBRE "REQUISITOS MÍNIMOS PARA LA GESTIÓN Y CONTROL DE LOS RIESGOS DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN"	Anexo a la Com. "A" 7724

-Índice-

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Sección 7. Infraestructura tecnológica y procesamiento.

7.1. Gestión de la infraestructura tecnológica.
7.2. Gestión de cambios.
7.3. Actualización de la infraestructura tecnológica.
7.4. Gestión de las comunicaciones.
7.5. Procesamiento de datos.
7.6. Gestión de copias de respaldo de datos.
7.7. Monitoreo de la infraestructura tecnológica y procesamiento.

Sección 8. Gestión de ciberincidentes.

8.1. Preparación de la respuesta ante ciberincidentes.
8.2. Ejercicios y pruebas de la respuesta ante ciberincidentes.
8.3. Control y reportes de gestión.

Sección 9. Desarrollo, adquisición y mantenimiento de “software”.

9.1. Requisitos para los sistemas y aplicaciones.
9.2. Gestión del ciclo de vida de “software”.

Sección 10. Gestión de la relación con terceras partes

10.1. Marco de gestión de la relación con terceras partes.
10.2. Formalización de la relación.
10.3. Control y monitoreo
10.4. Informes de auditoría interna y externa.

Sección 11. Canales Electrónicos.

11.1. Alcance.
11.2. Procesos de referencia.
11.3. Requisitos generales.
11.4. Escenarios de Canales Electrónicos.
11.5. Matriz de escenarios.
11.6. Glosario.
11.7. Tablas de requisitos técnico-operativos.

Sección 12. Glosario de términos.

Sección 1. Disposiciones generales

1.1. Sujetos obligados

1.1.1. Entidades Financieras

1.2. Aspectos generales

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

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

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

Adicionalmente las entidades deberán promover:

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

Sección 2. Gobierno de tecnología y seguridad de la información

Las entidades deberán establecer un marco de gobierno de la tecnología y seguridad de la información acorde con sus operaciones, procesos y estructura que permita el cumplimiento de los siguientes objetivos:

- Gestión integral y optimización de los recursos tecnológicos.
- Alineación con las necesidades del negocio.
- Supervisión adecuada de las actividades de tecnología de la información.
- Gestión de los riesgos relacionados con la tecnología y seguridad de la información.

A su vez, deberán establecer marcos de gestión que permitan lograr una coordinación de las actividades, con el fin de medir y comparar los resultados obtenidos con los objetivos propuestos.

2.1. Roles, responsabilidades y funciones de gobierno

Complementariamente a las disposiciones establecidas en los Textos Ordenados “Autoridades de Entidades Financieras”, “Lineamientos sobre Gobierno Societario en Entidades Financieras” y “Normas Mínimas sobre Controles Internos para Entidades Financieras”, las entidades deberán definir formalmente los roles y responsabilidades específicos para los niveles jerárquicos que se indican a continuación.

2.1.1. Directorio

El Directorio o autoridad equivalente de la entidad (Consejo de Administración, en el caso de entidades financieras cooperativas, o representante a cargo de primer nivel jerárquico, en el caso de sucursales de entidades financieras extranjeras), tendrá a su cargo las siguientes responsabilidades:

- Establecer y mantener componentes de gobierno coordinados con respecto a la autoridad y las responsabilidades para lograr la misión, las metas y los objetivos del negocio.
- Aprobar y supervisar las estructuras organizacionales y las políticas de alto nivel relacionadas con el marco de gobierno de la tecnología y seguridad de la información.
- Monitorear de manera continua el desempeño del gobierno de la tecnología y seguridad de la información, a fin de cumplir con las metas y objetivos establecidos.
- Impulsar y supervisar los proyectos estratégicos de tecnología y seguridad de la información.
- Asegurar la disposición de recursos adecuados y suficientes a las áreas relacionadas con la gestión de tecnología y la seguridad de la información.
- Aprobar y supervisar el marco de gestión de riesgos, y el apetito de riesgo de tecnología de la información.
- Fomentar una cultura de gestión de los riesgos de tecnología y seguridad de la información que abarque a toda la entidad.
- Promover la implementación de un marco de gestión de seguridad de la información y supervisar su efectividad.
- Aprobar el marco de gestión de continuidad del negocio y los mecanismos que aseguren la ciberresiliencia, y supervisar su desempeño.
- Aprobar las políticas para gestionar la relación con terceras partes.
- Aprobar las políticas para informar ciberincidentes significativos a las agencias gubernamentales.
- Aprobar políticas para informar acerca de los incidentes que comprometan datos de clientes.

2.1.2. Alta Gerencia

Las entidades deberán establecer las responsabilidades de la Alta Gerencia o Dirección Ejecutiva respecto de la tecnología y la seguridad de la información. La Alta Gerencia tendrá a cargo las siguientes responsabilidades:

- Diseñar estrategias y planes de tecnología de la información y definir el presupuesto necesario para cumplirlos.
- Conocer y comprender los riesgos relacionados con tecnología y seguridad de la información, asegurar que sean contemplados en los programas de gestión establecidos y definir planes de mitigación de los riesgos detectados.
- Diseñar estrategias, planes y medidas de seguridad de la información, y definir el presupuesto necesario para cumplirlos.
- Definir y asegurar la implementación y el mantenimiento de políticas de alto nivel.
- Definir los roles y responsabilidades necesarios para los procesos de tecnología y seguridad de la información de manera coordinada y eficaz.
- Establecer un marco de gestión de la seguridad de la información que permita asegurar la identificación, prevención, detección, respuesta y recuperación ante ciberincidentes.
- Implementar las prácticas de control interno y gestión de riesgos, y garantizar que las decisiones de tecnología de la información se tomen de acuerdo con el apetito de riesgo de la entidad.
- Delinear un marco de gestión de continuidad del negocio, sus documentos asociados y los informes resultantes.
- Definir e implementar un esquema de control y monitoreo continuo de los procesos, servicios y/o actividades delegadas en las terceras partes.
- Asegurar la gestión de los conocimientos, habilidades y capacidades de acuerdo con las tecnologías utilizadas.
- Establecer mecanismos de comunicación y coordinación entre las áreas de gestión de riesgos, tecnología y seguridad de la información para el cumplimiento de sus objetivos.
- Asegurar la incorporación en los proyectos de tecnología de la información el principio de seguridad desde el diseño.
- Asegurar la realización de evaluaciones de impacto y definición de apetitos de riesgo para la utilización de inteligencia artificial.
- Aprobar los protocolos de comunicación y las responsabilidades ante situaciones de escenarios de crisis y/o emergencia.
- Asegurar que los requerimientos vinculados a la protección de los usuarios de servicios financieros sean contemplados en los procesos de tecnología correspondientes.
- Aceptar los riesgos residuales derivados de la gestión de riesgos de tecnología y seguridad

La Alta Gerencia, ya sea que esté establecida en la República Argentina, en dependencias de la casa matriz o controlante económico, deberá mantener informado al Directorio respecto de los resultados de la gestión de tecnología y seguridad de la información, y el nivel de exposición a riesgos.

2.1.3. Áreas de tecnología y seguridad de la información

Los responsables de las áreas de gestión de tecnología y seguridad de la información deberán coordinar, monitorear e informar la ejecución de las actividades, en función a los lineamientos definidos por la Alta Gerencia. Estas funciones deberán ejecutarse en la República Argentina.

En los casos de entidades que cuenten con actividades descentralizadas en el exterior, estas funciones podrán reportar en forma directa:

- En Argentina, a la Alta Gerencia o la Dirección Ejecutiva.
- En dependencias de la Casa Matriz o Controlante Económico, a niveles jerárquicos que posean responsabilidades en materia de tecnología y seguridad de la información.

2.1.4. Comité de gobierno de tecnología y seguridad de la información.

Las entidades deberán definir al menos un comité de gobierno de tecnología y seguridad de la información. Este comité deberá estar integrado, al menos, por un miembro del Directorio o autoridad equivalente, miembros de la Alta Gerencia, y los responsables de las áreas de tecnología y seguridad de la información. A su vez, se deberá procurar la participación de funcionarios de alto nivel de las otras áreas de acuerdo con los temas a tratar.

Sus responsabilidades incluirán, como mínimo:

- Vigilar y evaluar el funcionamiento del marco de gestión de tecnología de la información y contribuir a la mejora de su efectividad.
- Vigilar y evaluar el funcionamiento del marco de gestión de seguridad de la información y la efectividad del mismo.
- Supervisar las definiciones, la priorización y el cumplimiento de los planes de tecnología y seguridad de la información.
- Supervisar la efectividad del marco de gestión de continuidad del negocio y los mecanismos que aseguren resiliencia tecnológica.
- Supervisar la ejecución de las acciones correctivas tendientes a regularizar o minimizar las observaciones surgidas de los informes de las auditorías sobre los aspectos de tecnología y seguridad de la información.
- Monitorear los resultados del marco de gestión de riesgos relacionados con tecnología y seguridad de la información y verificar que los planes de mitigación sean ejecutados de acuerdo con los cronogramas definidos.
- Supervisar la gestión integral de ciberincidentes y los reportes asociados.
- Mantener informado al Directorio de los temas tratados y las decisiones tomadas.

Este comité deberá reunirse con una periodicidad mínima que resulte acorde a sus operaciones, procesos y estructura. Se deberán elaborar actas formales de cada reunión mantenida en donde constará el detalle de los temas tratados, así como las acciones para su seguimiento posterior.

2.2. Segregación de funciones

Las entidades deberán establecer formalmente una delimitación de roles y responsabilidades que mitigue los riesgos asociados a una superposición de funciones y a la inexistencia de controles por oposición de intereses. Esta definición deberá ser extensible a los roles y responsabilidades delegados en las terceras partes.

Las funciones relacionadas con el gobierno y la gestión de la tecnología y seguridad de información no podrán ser acumuladas con las funciones vinculadas con: Recursos Humanos, Relaciones Institucionales, Administración Contable, Gestión Financiera, Gestión Comercial, Marketing, Gestión de Riesgo Integral y Auditoría Interna.

Cuando las áreas relacionadas con tecnología y seguridad de la información asuman funciones de la primera y la segunda línea, las entidades deberán documentar los riesgos derivados de la falta de independencia de la segunda línea.

En aquellos casos excepcionales, en que no pueda segregarse alguna de las funciones, el Directorio deberá asumir formalmente el riesgo y deberá evidenciarse la existencia formal y documentada de controles compensatorios realizados por sectores independientes.

2.3. Marco normativo

Las entidades deberán establecer un marco normativo formalizado que incluya las políticas, normas y procedimientos para la gestión efectiva, la supervisión y el control de los procesos de gestión de riesgos, tecnología, seguridad de la información, la continuidad del negocio, la gestión de ciberincidentes y la gestión de terceras partes.

Se deberán implementar mecanismos para su publicación y comunicación formal a todos los involucrados, tanto de la entidad, como de terceras partes. Además, se deberá establecer un proceso para su estandarización y actualización periódica.

Sección 3: Gestión de riesgos de tecnología y seguridad de la información

Las entidades deberán establecer un área o una función de gestión de riesgos relacionados con tecnología y seguridad de la información, en correspondencia con los textos ordenados sobre “Lineamientos para la Gestión de Riesgos en las Entidades Financieras” y “Agregación de Datos sobre Riesgos y Elaboración de Informes”.

Esta área o función deberá formar parte de la unidad responsable de la gestión de riesgo operacional y ser independiente de las áreas que originan los riesgos, de las líneas de negocios y de la auditoría interna. Tendrá, entre otras, las siguientes responsabilidades:

- Coordinar la definición, implementación y actualización del marco metodológico.
- Definir, revisar y actualizar periódicamente el marco de gestión de los riesgos de tecnología y seguridad de la información.
- Asegurar la identificación, evaluación, seguimiento, control, mitigación, y comunicación de los riesgos de tecnología y seguridad de la información.
- Mantener información actualizada y disponible para la toma de decisiones.
- Promover una cultura de gestión de riesgos de tecnología y seguridad de la información y brindar capacitación alineada a los objetivos.

El marco para la gestión de riesgos de tecnología y seguridad de la información deberá estar alineado con las políticas y prácticas establecidas para la gestión integral de riesgos. En dicho marco las entidades deberán:

- Determinar la tolerancia al riesgo en función del apetito de riesgo establecido.
- Establecer las políticas y la metodología para la gestión de riesgos.
- Establecer procedimientos para la identificación y evaluación de los riesgos. que incluya los vinculados a las terceras partes.
- Establecer procedimientos para el tratamiento de los riesgos y evaluar su efectividad.
- Formalizar y someter a aprobación los riesgos residuales derivados de la gestión de riesgos de tecnología y seguridad.
- Realizar un monitoreo continuo de los niveles de exposición a riesgos de tecnología y seguridad de información.
- Establecer indicadores vinculados con la gestión de los riesgos.
- Establecer que se comunique al Directorio y a los comités correspondientes los resultados de la gestión.

Las áreas de tecnología y seguridad de la información serán responsables de efectuar la identificación de los riesgos, y la definición técnica e implementación de las medidas de tratamiento.

La entidad deberá asegurar que el marco para la gestión del riesgo esté sujeto a un proceso de auditoría interna y externa. Además, se podrá involucrar a otros terceros independientes debidamente calificados.

Dentro de los riesgos relacionados con la tecnología y seguridad de la información incluidos en la evaluación, se deberán considerar especialmente los relacionados con:

- Escenarios que afecten la resiliencia tecnológica.
- La obsolescencia de la tecnología y los sistemas.
- La gestión de la relación con terceras partes.
- El desarrollo y utilización de algoritmos de inteligencia artificial o aprendizaje automático.
- La adopción de tecnología nueva o emergente.
- Software o aplicaciones utilizadas por usuarios que no fueron formalmente autorizados.

- Los aspectos de protección de datos personales en el uso de tecnologías de registros distribuidos (Distributed Ledger Technology - DLT).
- Escenarios de ciberincidentes relacionados con datos personales.

Adicionalmente, se deberán realizar evaluaciones de riesgos específicas:

- Antes del lanzamiento de nuevos productos o servicios que originen cambios importantes en los sistemas de información, en los procesos, servicios y/o actividades de tecnología y seguridad de la información.
- Antes de la delegación en terceras partes de procesos, servicios y/o actividades.

Sección 4: Gestión de tecnología de la información

4.1. Estrategia de tecnología de la información

Las entidades deberán establecer una estrategia de tecnología de la información, acorde a sus operaciones, procesos y estructura, que permita lograr una alineación entre los resultados de la gestión de tecnología de la información, y los requerimientos del negocio y de seguridad.

Para ello, se deberán considerar los resultados de la gestión de riesgos y los objetivos de la estrategia de seguridad. Adicionalmente, las entidades deberán:

- Establecer objetivos estratégicos y metas vinculados con la estrategia de tecnología de la información.
- Definir planes de acción que incluyan las medidas a adoptar para lograr el objetivo de la estrategia de tecnología de la información.
- Revisar los planes de acción regularmente para garantizar que sean relevantes y apropiados.
- Establecer procesos para realizar el seguimiento y medir la eficacia de la aplicación de su estrategia de tecnología de la información.

4.2. Arquitectura empresarial

De acuerdo con sus operaciones, procesos y estructura, las entidades deberán establecer un modelo de arquitectura empresarial que permita coordinar la estrategia de datos, la arquitectura de tecnología y aplicaciones con los procesos del negocio. Se deberán incluir principios, estándares y prácticas para:

- Brindar soporte al Directorio y la Alta Gerencia en la toma de decisiones respecto de las inversiones en tecnología.
- Favorecer la evaluación de las medidas de seguridad de la información, resiliencia operacional, gestión de datos, conectividad externa y la alineación con los objetivos de la entidad.
- Gestionar la complejidad del entorno del negocio y la tecnología con el fin de mejorar el impacto de los cambios en la organización.
- Favorecer la interoperabilidad e integración con servicios propios o de terceras partes.
- Comparar la arquitectura existente con los objetivos a largo plazo, las necesidades futuras y los cambios planificados.

4.3. Presupuesto, inversiones y gestión de portafolio

Las entidades deberán establecer prácticas efectivas para la elaboración de los presupuestos de tecnología de la información y para la evaluación continua de las inversiones realizadas. Se deberán establecer canales de comunicación formales para notificar oportunamente los desvíos en su ejecución.

Además, las áreas de tecnología de la información, junto con las áreas de negocio, deberán definir e implementar un proceso de gestión de portafolio que permita capturar, evaluar, priorizar, programar y ejecutar los requerimientos del negocio. Este proceso deberá tener en cuenta los siguientes objetivos:

- Contribuir a la planificación estratégica de tecnología de la información, de acuerdo con las necesidades del negocio.
- Proveer la información necesaria para la planificación de actividades tomando en consideración los proyectos, los recursos, costos y prioridades.
- Rendir cuentas respecto de la utilización del presupuesto de tecnología.

Los procesos establecidos deberán estar alineados con la estrategia de tecnología de la información, la arquitectura empresarial, el proceso de gestión de presupuesto y la gestión de proyectos.

4.3.1. Gestión de proyectos

Las entidades deberán establecer un marco para la gestión de proyectos que alcance todo su ciclo de vida y asegure su alineación con los objetivos estratégicos de la entidad. Se deberán definir estándares que incluyan:

- La asignación de roles y responsabilidades para la dirección, ejecución y supervisión de las actividades.
- La definición de las metodologías de gestión de proyectos utilizadas.
- La evaluación de los riesgos de todo el ciclo de vida, en concordancia con lo establecido en la Sección 3: Gestión de riesgos de tecnología y seguridad de la información.
- Criterios para el seguimiento y la comunicación de los desvíos y riesgos.
- La documentación y los reportes de gestión a elaborar.

Se deberán elaborar planes detallados para todos los proyectos de tecnología de la información, que incluyan, entre otros aspectos: la definición de alcances, actividades, hitos, resultados esperados para cada fase, roles y responsabilidades de los participantes. Adicionalmente, cuando el proyecto incluya el desarrollo o adquisición de software deberán contemplarse los requisitos de la Sección 9. Desarrollo, adquisición y mantenimiento de software.

Cuando no sea posible delimitar las funciones involucradas en alguno de los proyectos, se deberán considerar las exigencias establecidas en la Sección 2. Gobierno de tecnología y seguridad de la información respecto de la segregación de funciones.

Las entidades deberán notificar a la Gerencia de Auditoría Externa de Sistemas aquellos proyectos que involucren la implementación de nuevos servicios financieros digitales o cambios en la modalidad de los servicios existentes, cuando traten datos de clientes y de usuarios de servicios financieros, datos contables y/o transaccionales.

4.4. Gestión de datos

Las entidades deberán definir un proceso que establezca responsabilidades, políticas y procedimientos para la gestión de datos, que abarque todas las etapas de su ciclo de vida y sea acordes a sus operaciones, procesos y estructura.

La gestión de datos deberá estar alineada con la estrategia de negocio, la arquitectura empresarial, y el marco de gestión de seguridad de la información. Además, deberá establecer criterios para:

- Identificar los datos, tanto estructurados, como no estructurados.
- Controlar el uso de los datos en las actividades de la entidad y las terceras partes.
- Asegurar la gestión de la calidad del dato durante todo el ciclo de vida.
- Definir las necesidades para la conservación, el almacenamiento y la realización de copias de respaldo de los datos en función de la clasificación.

- Disponer la eliminación de los datos al final de su ciclo de vida de manera que se impida su recuperación.
- Supervisar el cumplimiento de las políticas y procedimientos de gestión de datos.
- Controlar la ejecución de los proyectos y servicios de gestión de datos.

Adicionalmente, se deberán establecer procesos y procedimientos para la obtención y la identificación de los datos tratados por la entidad que consideren, como mínimo, los datos de clientes, datos contables y datos transaccionales. Además, se deberán definir mecanismos para el intercambio de estos tipos de datos con otras entidades o terceras partes.

4.4.1. Clasificación de los datos e información

Las entidades deberán definir políticas y procedimientos para la clasificación de los datos e información en concordancia con la gestión de datos, que considere:

- La participación del propietario del dato o la información.
- Los criterios de integridad, disponibilidad, confidencialidad y valor para el negocio.
- La frecuencia y recurrencia del uso de los datos y la información, la modalidad, el formato y el tiempo durante el cual se debe almacenar.

4.5. Gestión de activos de información

Las entidades deberán definir un proceso que establezca responsabilidades, políticas y procedimientos para la gestión de los activos de información que brindan apoyo al negocio y a los servicios de la entidad, tanto propios, como delegados en terceras partes. Entre otros aspectos, se deberán considerar:

- La definición de criterios para la toma de decisiones relativas a la gestión de activos.
- El mantenimiento, el uso y la obsolescencia.
- Vulnerabilidades y necesidades de actualización o reemplazo.
- Cumplimiento con estándares internos de configuración y de seguridad.

Las entidades deberán mantener un inventario detallado y actualizado de sus activos de información, acorde con los objetivos y la política de gestión de activos. Los inventarios deberán contener información que permita identificar, como mínimo, aspectos referidos a:

- La identificación de los propietarios de los activos de información.
- La ubicación, la configuración, las interconexiones internas y externas, y las interdependencias de cada uno de los activos de información.
- La clasificación del activo considerado.

Por otra parte, se deberá definir un proceso para la clasificación de los activos de información, en concordancia con la clasificación de los datos requerida en el apartado precedente. La clasificación deberá mantenerse actualizada durante todo el ciclo de vida de los activos de información y deberá ser revisada cuando se produzcan cambios en los procesos, sus propietarios u otros cambios organizativos.

4.6. Inteligencia artificial o aprendizaje automático

Las entidades deberán identificar y documentar el objetivo del uso, por sí o por terceros, de software que utilice algoritmos de inteligencia artificial o aprendizaje automático en sus proyectos o procesos. Además, deberán establecer roles y responsabilidades para la definición del contexto en que operan los sistemas de inteligencia artificial o aprendizaje automático, la identificación de los modelos, algoritmos y los conjuntos de datos utilizados, y la definición de métricas y umbrales precisos para evaluar la confiabilidad de las soluciones implementadas.

Los análisis de riesgos correspondientes deberán considerar, como mínimo:

- Los modelos adoptados, su entrenamiento y las posibles discrepancias con la realidad del contexto;
- Los datos utilizados para el entrenamiento, su volumen, complejidad y obsolescencia.
- La privacidad y la afectación a los usuarios en su calidad de consumidores.
- El nivel de madurez de los estándares de pruebas de software y las dificultades para documentar las prácticas basadas en IA.

Adicionalmente, se deberán implementar procesos que promuevan la confiabilidad en el uso de este tipo de algoritmos e incluyan al menos:

- Medidas para evitar la existencia de sesgos o discriminación contra grupos o segmentos de clientes o usuarios de los productos y/o servicios financieros.
- Documentación respecto de la transparencia, la explicabilidad de los modelos utilizados y la interpretabilidad de los resultados.
- La ejecución de revisiones periódicas de los resultados respecto de la tolerancia al riesgo definida.
- La comunicación al cliente cuando utilice servicios soportados por este tipo de tecnología.

4.7. Control y reportes de gestión

Las entidades deberán definir un proceso de control sobre la gestión de las áreas de tecnología de la información, mediante procedimientos, herramientas y métricas que permitan realizar un seguimiento y evaluación de las tareas desarrolladas y del cumplimiento de objetivos. Asimismo, deberán incluir la identificación de oportunidades de mejora.

Las métricas deberán incluir indicadores o umbrales que permitan controlar los desvíos respecto de lo planificado, tanto para las tareas operativas, como de gestión, y establecer planes de acciones correctivas cuando sea necesario.

De acuerdo con sus operaciones, procesos y estructura, las entidades deberán promover la implementación de indicadores automatizados, como así también la generación de alertas ante la superación de umbrales.

El monitoreo de la efectividad de la gestión deberá considerar los resultados de los ejercicios de respuesta y recuperación ante ciberincidentes, y de la gestión de vulnerabilidades. Adicionalmente, se deberán evaluar los resultados de las actividades de mejora continua.

Los reportes de gestión de las áreas de tecnología deberán considerar las evaluaciones sobre la eficacia de los procesos que incluyan, al menos:

- El monitoreo de la capacidad en materia de comunicaciones, procesamiento, virtualización, hardware.
- Información sobre el rendimiento de los sistemas (disponibilidad, tiempos de respuesta y procesamiento).
- La gestión de cambios.
- La evaluación del cumplimiento de los acuerdos de nivel de servicios, incluidos los brindados por terceros.
- Los avances, desvíos y riesgos relevantes de los proyectos.
- La supervisión de los planes de acción ante incumplimientos o desvíos de la gestión.
- La gestión de la infraestructura tecnológica.

Además, se deberá establecer la frecuencia y los canales formales de comunicación de los resultados de la gestión de las áreas al Directorio y la Alta Gerencia.

Sección 5: Gestión de seguridad de la información

5.1. Marco de gestión de seguridad de la información

Las entidades deberán establecer un marco de gestión de la seguridad de la información que contemple:

- Los objetivos estratégicos del negocio y de tecnología, la gestión del dato, la clasificación de datos e información, los activos de información y los riesgos.
- La protección de los activos de información para asegurar la prestación de los servicios y contener el impacto de los eventos de seguridad.
- La identificación y detección de eventos que podrían dar lugar a un ciberincidente, y el diseño e implementación de medidas para responder de manera planificada y oportuna.
- El diseño de medidas destinadas a brindar seguridad de la información a los procesos y servicios en la recuperación ante ciberincidentes.

5.2. Estrategia de seguridad de la información

Las entidades deberán definir una estrategia de seguridad de la información alineada con la estrategia del negocio y acorde a sus operaciones, procesos y estructura. Deberá ser consistente con la estrategia de tecnología de la información, la arquitectura empresarial y los resultados de la gestión de riesgos de tecnología y seguridad. Asimismo, deberá considerar:

- Las amenazas y las vulnerabilidades asociadas a cada entorno tecnológico, su impacto en el negocio y los estándares internacionales vigentes.
- Los recursos humanos y tecnológicos propios de la entidad.
- Requerimientos de los organismos de regulación y control, y otros entes externos vinculados directa o indirectamente.
- Las dependencias de terceras partes.

En la elaboración de la estrategia, las entidades deberán:

- Establecer los objetivos estratégicos y metas para la gestión de proyectos y para los procesos de seguridad de la información, incluidas las necesidades de capacitación y concientización.
- Crear planes de acción que incluyan las medidas para lograr los objetivos de la estrategia de seguridad de la información.
- Considerar la gestión de amenazas y vulnerabilidades, y la clasificación de datos e información y de los activos de información.
- Definir objetivos y lineamientos para los procesos de detección de eventos y amenazas.
- Considerar la gestión de ciberincidentes.

5.3. Normas y procedimientos

Las entidades deberán establecer como parte del marco normativo, normas y procedimientos que permitan gestionar, controlar y documentar las actividades de los procesos para la gestión de la seguridad de la información. Deberán incluirse, como mínimo, los referidos a:

- Control de accesos.
- Contraseñas.
- Gestión de vulnerabilidades.
- Detección y monitoreo.
- Criterios para compartir información referida a amenazas y vulnerabilidades.
- Dispositivos de la entidad asignados a los usuarios.
- Dispositivos propios del usuario utilizados en la entidad.
- Modelado de amenazas.
- Aspectos específicos de desarrollo seguro de acuerdo con las metodologías utilizadas.
- Detección y regularización de software de usuario no autorizado.
- Estándares de informática forense.

Además, de acuerdo con sus operaciones, procesos y estructura, las entidades deberán establecer estándares de seguridad que aborden los siguientes aspectos, como mínimo:

- La implementación de configuraciones seguras.
- La adopción, revisión e implementación de algoritmos de criptografía.

5.4. Presupuesto, inversiones y gestión de proyectos

Las entidades deberán establecer prácticas efectivas para la elaboración de los presupuestos de seguridad de la información y para la evaluación continua de las inversiones realizadas. Se deberán establecer canales de comunicación formales para notificar oportunamente los desvíos en su ejecución.

Se deberán elaborar planes detallados para todos los proyectos que incluyan, entre otros aspectos: la definición de alcances, actividades, hitos, resultados esperados para cada fase, roles y responsabilidades de los participantes. La definición de alcances deberá ser consistente con las necesidades de negocio y estar alineada con los proyectos estratégicos del negocio y de tecnología, la arquitectura empresarial y el modelo de gestión de datos.

5.5. Programas de capacitación y concientización

Las entidades deberán establecer programas de capacitación y concientización en materia de seguridad de la información, medibles y verificables, que alcancen a toda la organización, terceros, clientes y usuarios de servicios financieros. Estos programas deberán contemplar los riesgos de tecnología y seguridad de la información, y los aspectos relacionados con la gestión de ciberincidentes.

Para la definición de los objetivos de los programas y planes de capacitación y concientización se deberán contemplar, al menos:

- Contenidos mínimos a desarrollar, plazos y público alcanzado.
- La vinculación con los planes de seguridad de la información.
- La incorporación de lecciones aprendidas en ciberincidentes previos, o a través de pruebas y ejercicios.
- La publicación actualizada de información de seguridad para los clientes y usuarios de servicios financieros.

Para el desarrollo de los planes deberán tenerse en cuenta, como mínimo, los siguientes aspectos:

- Segmentación de públicos y elaboración de contenidos específicos que incluyan:
    - Para usuarios internos y de terceros, el marco normativo y las prácticas de seguridad aplicables.
    - Para clientes y usuarios de servicios financieros, las prácticas de seguridad de la información necesarias para el uso seguro de los servicios que brinde la entidad.
- La actualización permanente en función de los resultados de la gestión de vulnerabilidades y ciberincidentes.

Los programas de capacitación y concientización deberán ser revisados con una periodicidad mínima anual, con el objetivo de evaluar e informar a la Alta Gerencia acerca de la efectividad de las actividades realizadas.

El contenido de los planes de capacitación destinados a los usuarios internos y de terceros deberán considerar, al menos:

- Los riesgos en el uso de dispositivos propios en la organización.
- Los riesgos en el uso de dispositivos asignados por la entidad.
- Los aspectos específicos de la metodología de desarrollo seguro.
- Los riesgos en el uso de software o aplicaciones no autorizadas.
- Los riesgos de la incorporación de tecnologías no autorizadas (shadow IT).

5.6. Control y reportes de gestión

Las entidades deberán definir un proceso de control sobre la gestión de las áreas de seguridad de la información, mediante procedimientos, herramientas y métricas que permitan realizar un seguimiento y evaluación de las tareas desarrolladas, y del cumplimiento de objetivos. Asimismo, deberán incluir la identificación de oportunidades de mejora.

Las métricas deberán incluir indicadores o umbrales que permitan controlar los desvíos respecto de lo planificado, tanto para las tareas operativas, como de gestión, y establecer planes de acciones correctivas cuando sea necesario. Adicionalmente, se deberán evaluar los resultados de las actividades de mejora continua.

De acuerdo con sus operaciones, procesos y estructura, las entidades deberán promover la implementación de indicadores automatizados, como así también la generación de alertas ante desvíos respecto de los umbrales.

Los reportes de gestión de las áreas de seguridad de la información deberán considerar especialmente las evaluaciones sobre la eficacia de los procesos que incluyan, al menos:

- Resultados de la gestión de respuesta y recuperación ante ciberincidentes y de los ejercicios.
- Control de accesos.
- Operaciones de seguridad.
- Gestión de vulnerabilidades.
- Evaluación de los acuerdos de nivel de servicios, incluidos los brindados por terceros.
- Supervisión de los planes de acción ante incumplimientos o desvíos de la gestión.

Además, se deberá establecer la frecuencia y los canales formales de comunicación de los resultados de la gestión de las áreas al Directorio y la Alta Gerencia.

5.7. Control de accesos físico, a sistemas y a datos

5.7.1. Seguridad física y medioambiental

Las entidades deberán diseñar e implementar controles que les permitan evitar la existencia de puntos únicos de falla y mitigar los riesgos vinculados con la seguridad física de las áreas destinadas al procesamiento, la transmisión y el almacenamiento de información para evitar accesos no autorizados o detectarlos. Se deberán establecer procedimientos para:

- El mantenimiento preventivo y la realización de pruebas periódicas de los dispositivos de control ambiental y de los equipos de energía redundantes.
- La aplicación de técnicas para la destrucción de activos acorde con su clasificación.
- La autorización y el registro del retiro y el traslado de activos desde las instalaciones.
- El monitoreo permanente de la efectividad de las medidas de protección implementadas.

Las medidas de prevención, detección y corrección establecidas deberán estar alineadas con los resultados de los análisis de riesgos de tecnología y seguridad de la información, los estándares y buenas prácticas. Además, deberán incluir, como mínimo:

- Instalaciones de montaje adecuadas para los sistemas de suministro eléctrico y medidas para la redundancia de la energía eléctrica.
- Medidas para controlar los niveles de temperatura y humedad ambiental.
- Uso de materiales constructivos no inflamables o ignífugos.
- Alarmas y sistemas para la detección y extinción de incendios.
- Sistemas de video y grabación de eventos.
- Sistemas para el control de accesos a las instalaciones que permitan la segregación de permisos y el registro de los ingresos.
- Sistemas para el monitoreo y control de las medidas de protección implementadas;
- Medidas para controlar la exposición de las estaciones de trabajo, dispositivos de comunicaciones y de red.

5.7.2. Control de accesos y gestión de privilegios

En concordancia con la política de seguridad de la información, las entidades deberán definir un proceso de gestión que permita solicitar, aprobar, asignar, modificar, monitorear y revocar los derechos de acceso a los activos de información. Este proceso deberá:

- Alcanzar a todos los activos de información, incluido el acceso físico a las instalaciones de los centros de procesamiento, almacenamiento y transmisión de datos.
- Asegurar la aplicación de los principios de segregación de funciones y mínimos privilegios.
- Identificar las funciones que requieren la intervención de más de un usuario y definir los controles pertinentes.
- Establecer criterios para la asignación de derechos de acceso acordes con los roles, funciones y las responsabilidades del personal de la entidad y de terceras partes.
- Asegurar la adecuación oportuna de los derechos de acceso y privilegios de los usuarios en función de los cambios de puestos de trabajo o las desvinculaciones.
- Establecer circuitos para la autorización de accesos y privilegios que cuenten con la participación de los propietarios de los activos de información.
- Identificar y revocar las cuentas expiradas, inactivas o que incumplan las políticas de seguridad.
- Definir revisiones periódicas de los niveles de acceso y los privilegios asignados sobre los activos de información, con la participación de los propietarios de activos de información.
- Establecer procedimientos para la asignación y el monitoreo del uso de cuentas genéricas, privilegiadas y de servicio.
- Implementar controles automatizados sobre las funciones de creación, modificación, habilitación, revocación y eliminación de cuentas.

Las entidades deberán implementar medidas que permitan mantener el control sobre las cuentas privilegiadas y de servicio. Entre otros, deberán:

- Establecer y mantener un inventario de cuentas de servicio y privilegiadas.
- Restringir los accesos de administración a cuentas privilegiadas.
- Implementar controles sobre cuentas por defecto para evitar su uso no autorizado.
- Promover la implementación de autenticación multifactor para las cuentas privilegiadas.
- Utilizar procesos y herramientas para administrar la asignación de derechos de acceso sobre las cuentas privilegiadas y de servicio.

Las entidades deberán implementar medidas que permitan mantener el control sobre los derechos de acceso asignados. Entre otros, y de acuerdo con sus operaciones, procesos y estructura, deberán considerar:

- Automatización del proceso de creación, habilitación, modificación, revocación y eliminación de cuentas de usuario.
- Notificaciones automáticas de los cambios.
- Procesos de administración dinámica de privilegios.

Se deberán implementar mecanismos que aseguren que las actividades de todas las cuentas se identifiquen y registren de manera única, y brinden información suficiente para fines de auditoría e investigación.

5.7.2.1. Medidas de control de acceso

Las entidades deberán establecer directivas de seguridad para el acceso a los activos de información basadas en la gestión de vulnerabilidades y amenazas, y en la clasificación de activos de información. Estas directivas deberán definir, como mínimo, los métodos utilizados para la autenticación.

Además, deberán definir modelos de accesos para los usuarios que contemplen los factores de autenticación, el comportamiento en el uso de servicios y distintas fuentes de información que permitan validar su identidad.

Las entidades deberán establecer procedimientos para:

- La implementación, revisión periódica y actualización de las reglas de control de acceso a los dispositivos de red, que aseguren que las mismas se mantienen actualizadas.
- El establecimiento de controles que permitan detectar y evitar la conexión de dispositivos no autorizados en las redes.
- La gestión e implementación de métodos de autenticación en los servicios de intercambio de información con terceras partes.
- La implementación de medidas para la seguridad de las conexiones de acceso remoto, los dispositivos habilitados y la información accedida o utilizada.

5.7.2.2. Métodos de autenticación

Para la selección e implementación de los métodos de autenticación y sus factores las entidades deberán considerar los resultados de los análisis de riesgos, y el cumplimiento de las políticas y los procedimientos de control de acceso.

En la definición e implementación de las especificaciones técnicas de los métodos de autenticación deberán considerarse: los factores de autenticación, la validación y el canal utilizado. Se deberán establecer medidas de protección que aseguren la integridad y confidencialidad de los factores de autenticación durante todo su ciclo de vida. En particular, las entidades deberán:

- Implementar medidas adicionales para resguardar la confidencialidad en los datos de autenticación que deban ser secretos del cliente o usuario del servicio.
- Definir controles para evitar la pérdida, el robo o la duplicación no autorizada.
- Establecer criterios y controles sobre los plazos de vencimiento de las credenciales.
- Evaluar la frecuencia en la presentación de los factores de autenticación junto a la gestión de sesiones.

5.7.2.3. Requisitos generales para los factores de autenticación

En la implementación de factores de autenticación, las entidades deberán aplicar los controles mínimos establecidos a continuación. Adicionalmente, y en función de los resultados de los análisis de riesgos, y la gestión de amenazas y vulnerabilidades, podrán aplicarse controles complementarios.

Secreto memorizado: Para el uso seguro de secretos memorizados, las entidades deberán establecer requisitos mínimos y controles que incluyan:

- Establecer una longitud mínima y reglas de composición acorde con los riesgos específico del servicio.
- Permitir la concatenación de varias palabras para crear secretos largos.
- Limitar el uso de datos del usuario o de su contexto que sean fácilmente adivinables (como nombres o fechas).
- Restringir la reutilización de secretos previamente empleados por el usuario.
- Brindar funcionalidad que permita la sustitución cuando existe sospecha de que han sido comprometidos.
- Definir el tiempo de vigencia y expiración.
- Revocar las contraseñas de más de un año de antigüedad.
- Limitar el número máximo de intentos fallidos de autenticación, y establecer un mecanismo de conteo y bloqueo tras alcanzar el máximo.
- Usar un canal protegido en el proceso de verificación.
- Establecer medidas para la seguridad de los secretos almacenados que reduzcan el riesgo de ataques fuera de línea, incluyendo el uso de algoritmos de hash o cifrado.
- Establecer controles que limiten la utilización de secretos fácilmente deducibles, ampliamente utilizados o previamente comprometidos.

Autenticación fuera de banda: Las entidades deberán considerar la implementación de los siguientes controles mínimos:

- El uso de un canal de comunicación distinto y cifrado para el envío de mensajes de autenticación.
- La utilización de métodos que prueben la posesión y el control sobre el dispositivo.

La autenticación fuera de banda mediante SMS debe tener un uso restringido, acorde a los riesgos asociados y requiere la aplicación de controles complementarios.

Dispositivos criptográficos o almacén de claves criptográficas: Para el uso seguro de dispositivos criptográficos o de almacén de claves criptográficas, las entidades deberán considerar la implementación de, al menos, los siguientes controles:

- Las claves se almacenarán de forma segura y no se permitirá su extracción.
- El requerimiento de la intervención del usuario para el uso del dispositivo o almacén de claves criptográficas.
- Medidas de protección fuertes sobre las claves.
- La utilización de algoritmos seguros para la generación de las claves.

Generación de claves de un solo uso (OTP): En su empleo, se deberá considerar, como mínimo la aplicación de los siguientes controles:

- La implementación de medidas de protección fuertes sobre las claves conservadas por la entidad.
- El uso de algoritmos criptográficos seguros para generar, intercambiar u obtener los datos en la asociación del dispositivo con la cuenta del usuario.
- El uso de canales protegidos y autenticados para la presentación de los códigos.

- La definición de un tiempo de vida para cada valor generado.
- El uso por única vez de cada valor generado.
- La limitación de intentos fallidos de ingreso de los códigos.
- Uso de algoritmos seguros para la generación de las claves.
- Definición de una longitud de semilla que asegure la generación de valores únicos durante toda la vida del dispositivo.

Uso de datos biométricos: En la implementación de métodos de autenticación que utilicen datos biométricos, se deberán evaluar y mitigar los riesgos derivados de las siguientes características:

- Las limitaciones para asegurar la autenticación del suscriptor debido al carácter probabilístico del método, la tasa de falsos positivos (FMR) y la falta de secreto del dato biométrico.
- La necesidad de establecer un proceso para la revocación de credenciales de este tipo.
- Las posibles vulnerabilidades en los dispositivos y sistemas utilizados para la captura y validación de las credenciales.
- El impacto en la privacidad de los usuarios.

Además, de acuerdo con la clasificación de los datos, la información y los activos a los que se brinde acceso, se deberán implementar controles que incluyan:

- El uso combinado con al menos un factor de autenticación adicional de otro tipo.
- El uso de canales protegidos para la transmisión (transferencia) de información.
- La definición de umbrales de confianza.
- La implementación de controles que mitiguen el riesgo de ataques en la etapa de presentación de credenciales.
- La aplicación de controles de intentos fallidos de autenticación.
- La aplicación de medidas que permitan la identificación de los dispositivos utilizados para la captura y validación de las credenciales.

5.7.2.4. Requisitos generales para la autenticación multifactor

Las entidades deberán evaluar la utilización de autenticación multifactor para el acceso a los activos de información de acuerdo con su clasificación, y la gestión de amenazas y vulnerabilidades. Además, las entidades deberán evaluar la robustez del método en conjunto con la usabilidad y la eficiencia.

En la implementación de autenticación multifactor se deberá utilizar al menos dos factores de distinta categoría o un autenticador multifactor.

Se considerará autenticador multifactor al software o hardware de generación de claves de un solo uso (OTP), o dispositivos criptográficos, cuando cumpla con los siguientes requisitos:

- El acceso al generador deberá requerir un factor de autenticación del tipo secreto memorizado o datos biométricos.
- Cuando se utilice un secreto memorizado para el acceso, éste deberá tener al menos 6 caracteres.

- Si se usan factores biométricos, se deberán tomar en cuenta las consideraciones del apartado anterior.
- Se deberán limitar los intentos fallidos de acceso.

5.7.3. Seguridad de los dispositivos portátiles

Se deberán establecer controles de seguridad para los dispositivos propios de la entidad asignados a los usuarios internos de acuerdo con la clasificación de los datos y la información, así como la gestión de vulnerabilidades y amenazas, que contemplen, como mínimo:

- Las configuraciones de seguridad de los dispositivos.
- El cifrado de la información.
- La limitación de instalación de software no autorizado.

Asimismo, se deberán implementar controles de seguridad para limitar la conexión y el acceso a las redes, sistemas e información a los dispositivos propios de los usuarios internos o contratistas.

5.7.4. Controles sobre la información

En concordancia con la clasificación de los datos y la información, y la gestión de las vulnerabilidades y amenazas, las entidades financieras deberán implementar medidas que les permitan detectar y evitar el acceso, la modificación, copia o transmisión no autorizada de información. Los controles implementados deberán:

- Cifrar la información en tránsito, almacenada en los sistemas, o en los dispositivos de los usuarios, en concordancia con su clasificación.
- Segmentar el procesamiento, la transmisión y el almacenamiento de la información.
- Establecer medidas para limitar los derechos de acceso a los datos en entornos productivos.
- Establecer medidas para el enmascaramiento y la protección de datos en entornos no productivos, de acuerdo con los resultados de su clasificación.
- Aplicar medidas de borrado seguro para eliminar la información de los medios de almacenamiento, los sistemas y los dispositivos asignados a los usuarios antes de su descarte o reutilización.
- Implementar mecanismos para la protección ante código malicioso.

Además, las entidades deberán implementar controles para identificar la transferencia o procesamiento no autorizados de información clasificada como confidencial o crítica.

5.8. Operaciones de seguridad

5.8.1. Detección, monitoreo y análisis de eventos

Las entidades deberán establecer un proceso para el registro y el análisis de la información vinculada con eventos de seguridad de los sistemas, las redes y la infraestructura tecnológica. Este proceso deberá permitir la detección de anomalías y eventos, la identificación de incidentes, y la vinculación con el proceso de gestión de ciberincidentes de acuerdo con la clasificación de datos e información y la de activos de información. Además, se deberán considerar, al menos, las siguientes actividades:

- Recolectar, procesar, controlar y conservar los registros de los eventos y las actividades de los usuarios en los sistemas de información y de la infraestructura que los soporta.
- Definir medidas para la mejora continua del proceso.
- Establecer y revisar perfiles de comportamiento de los usuarios y sistemas de información que permitan identificar las actividades habituales.
- Correlacionar distintos eventos incluidos en los registros de actividad para identificar patrones de actividad sospechosa o inusual.

Como parte de este proceso, las entidades deberán definir:

- Métricas para la ejecución de las actividades de monitoreo de los sistemas y su alineación con la estrategia.
- Evaluaciones continuas de los riesgos y los controles en función del monitoreo.
- Frecuencias para la ejecución del monitoreo y para la evaluación de la efectividad de los controles.
- Acciones para validar que las políticas y los estándares de configuración están implementados y funcionan de manera consistente.
- Umbrales para la categorización y el tratamiento de alertas.
- Alertas para el uso de accesos privilegiados.
- Medidas tendientes a asegurar la disponibilidad, precisión y vigencia de los resultados del monitoreo.
- Controles para la protección de los registros de actividad con el fin de evitar accesos no autorizados.
- Medidas para la conservación de los registros de eventos y de auditoría.

5.8.2. Gestión de amenazas y vulnerabilidades

Las entidades deberán establecer un proceso para recolectar, procesar, analizar e interpretar información referida a amenazas mediante métodos proactivos y reactivos, que brinde información para la toma de decisiones vinculadas con la gestión de ciberincidentes.

Además, deberán implementar acciones para la detección y eliminación de perfiles no autorizados en las redes sociales, plataformas de comercio electrónico, entre otros.

Por otra parte, las entidades deberán establecer un proceso de gestión de vulnerabilidades para todos los sistemas y aplicaciones, propios o de terceras partes, acorde con la gestión de riesgos y vinculado con la gestión de incidentes, que contemple las siguientes actividades:

- Establecer puntos de contacto para la notificación de vulnerabilidades de los servicios tanto internos, como externos de la entidad.
- Realizar un análisis y una evaluación del impacto de las vulnerabilidades de seguridad publicadas o reportadas a la entidad, que afecten a sus activos de información.
- Establecer un plan y un cronograma de mitigación del riesgo de acuerdo con su criticidad.
- Definir las medidas alternativas de mitigación cuando no existan actualizaciones disponibles o su implementación implique un riesgo mayor.
- Brindar información oportuna al proceso de gestión de actualizaciones de seguridad, que incluya la criticidad de la vulnerabilidad.

Sección 6: Gestión de la continuidad del negocio

6.1. Marco de gestión de la continuidad

Las entidades deberán establecer un marco de gestión de la continuidad del negocio que considere:

- Las disposiciones vigentes sobre “Lineamientos para la Gestión de Riesgos en las Entidades Financieras”, “Agregación de Datos sobre Riesgos y Elaboración de Informes” y “Lineamientos para la respuesta y recuperación ante ciberincidentes (RRCI)”.
- Los principios para la resiliencia operacional.
- Los resultados de la gestión integral de riesgos, y el apetito por el riesgo definido.
- Los objetivos estratégicos del negocio.
- La gestión de la tecnología y la seguridad de la información, y el modelo de arquitectura empresarial.

Este marco de gestión deberá establecer como mínimo:

- Criterios para la realización de análisis de impacto y la definición de las estrategias de continuidad.
- Lineamientos para la elaboración de planes de recuperación.
- Medidas para la mejora continua del marco de gestión.
- Un programa de ejercicios y testeo alineado con los realizados en la gestión de ciberincidentes.
- Planes para la capacitación y concientización.
- La gestión de los recursos vinculados con este marco de gestión.

En función de las operaciones, procesos y estructura de la entidad, se deberá designar un área, sector o responsable de la coordinación de las actividades vinculadas con la gestión de la continuidad del negocio. Asimismo, se deberán definir roles y responsabilidades para las distintas actividades que conforman el marco de gestión.

6.2. Ciberresiliencia en la continuidad del negocio

Las entidades deberán establecer medidas proactivas en el diseño de las operaciones y procesos que les permitan mitigar el riesgo de eventos disruptivos y mantener la confidencialidad, integridad y disponibilidad.

De acuerdo con los objetivos estratégicos del negocio, los resultados de la gestión de riesgos y las lecciones aprendidas, se deberán aplicar medidas que fortalezcan las capacidades de recuperación ante eventos disruptivos de la entidad respecto de:

- Las instalaciones, la arquitectura tecnológica y la infraestructura.
- Los ciberataques.
- Las estrategias de resguardos de datos y los mecanismos de replicación.
- Disponibilidad de personal esencial.
- Servicios provistos por terceras partes, interconexiones y dependencias.
- Los suministros de energía y abastecimiento.
- La gestión de cambios de emergencias.

6.3. Análisis de impacto y evaluación de riesgos

Las entidades deberán considerar como base para la gestión de continuidad del negocio el análisis de impacto del negocio (BIA), los resultados de la gestión de riesgos de tecnología y seguridad de la información, y de la gestión integral de riesgos de la entidad.

El análisis de impacto del negocio y las evaluaciones de riesgos deberán ser revisadas periódicamente o ante cambios significativos en la entidad o en su contexto de operación.

6.3.1. Análisis de impacto del negocio

Las entidades deberán implementar un proceso para la elaboración de análisis de impacto del negocio (BIA) que involucre a todas las áreas de la entidad y permita definir las necesidades y prioridades de recuperación.

Este proceso deberá incluir:

- La definición de criterios para la evaluación del impacto relevantes para la resiliencia y la continuidad.
- La identificación de las actividades que soportan la prestación de los productos y servicios.
- La identificación de las interdependencias de los procesos.
- La identificación de las dependencias de los procesos respecto de terceras partes.
- La identificación de los posibles incidentes disruptivos y la evaluación de su impacto.
- Los objetivos de recuperación en relación con el tiempo y a la pérdida de datos. (RTO/RPO).
- La razonabilidad de los objetivos de recuperación
- La comunicación de los resultados obtenidos a la Alta Gerencia.

6.3.2. Evaluación de riesgos y escenarios

Las entidades deberán realizar evaluaciones periódicas de los riesgos de escenarios disruptivos. En concordancia con el marco establecido para la gestión integral de riesgos, se deberán establecer planes de tratamiento acordes al apetito de riesgo.

Se deberán analizar los riesgos asociados con la ubicación geográfica, la susceptibilidad a las amenazas y la proximidad con infraestructuras críticas de todas las instalaciones, incluidas las provistas por terceras partes. Además, para los escenarios que correspondan, se deberán evaluar las amenazas de interrupción que pudieran afectar de manera simultánea a los distintos sitios.

6.4. Estrategias de continuidad del negocio

Las entidades deberán desarrollar estrategias de continuidad del negocio para cumplir con los objetivos de resiliencia y recuperación definidos, en función de los escenarios de amenaza identificados y de los procesos de negocio.

En su alcance, se deberán considerar los siguientes puntos:

- Detalle de la infraestructura de tecnología de la información, recursos involucrados y facilidades de procesamiento.
- Esquemas de copia de seguridad, replicación y almacenamiento para la protección de datos.
- La existencia de entornos aislados de recuperación.
- Niveles de redundancia en la infraestructura de telecomunicaciones.

- Inclusión de los riesgos no tecnológicos (por ejemplo, riesgos de transacción, liquidez y reputación).

6.4.1. Planes de continuidad del negocio

En función de las estrategias definidas, las entidades deberán establecer e implementar planes para la continuidad del negocio que permitan continuar las operaciones durante el período de restablecimiento del servicio afectado.

Los planes deberán contemplar las estrategias de continuidad definidas e incluir, como mínimo:

- Los procedimientos para la declaración de una situación de crisis y los criterios para la activación de planes vinculados.
- La asignación de responsabilidades para la ejecución de planes de recuperación.
- Los procedimientos detallados de recuperación, la identificación de la infraestructura, los sistemas y componentes críticos, y su prioridad para la recuperación.
- Los procedimientos para el traslado de actividades esenciales a las ubicaciones alternativas.
- El establecimiento de canales de atención alternativos para los clientes.
- Medidas que aseguren la integridad y confidencialidad de la información crítica durante los procesos de recuperación.

En función de sus operaciones, procesos y estructura, las entidades deberán establecer procedimientos automatizados que permitan mitigar los riesgos asociados a los procesos de recuperación manuales.

6.4.2. Gestión de crisis y estrategias de comunicación

La entidad deberá designar responsables para la toma de decisiones y la elaboración de planes de gestión de crisis. Además, deberá establecer procedimientos ante situaciones de crisis que estén vinculados con la gestión de incidentes y consideren escenarios de disrupción.

Asimismo, deberán definir estrategias de comunicación que alcancen:

- A los participantes en la ejecución de los procedimientos, tanto de la entidad, como de terceros.
- A las autoridades que correspondan y a otros interesados.

Se deberán establecer procedimientos de comunicación que aseguren la notificación a las partes interesadas, la definición de listas de contactos, y la participación de las áreas técnicas en la definición del contenido de la comunicación.

6.5. Programa de capacitación y concientización

Las entidades deberán establecer un programa y planes de capacitación que alcance a toda la organización y considere, como mínimo, la resiliencia operacional, los objetivos de continuidad del negocio, el impacto de los posibles escenarios disruptivos, los roles y responsabilidades del personal, y las lecciones aprendidas.

Para el desarrollo de los planes que componen el programa se deberá tener en cuenta, como mínimo, la identificación y segmentación de públicos, incluyendo al Directorio, la Alta Gerencia y las áreas responsables de atención al cliente.

Los planes deberán ser revisados periódicamente, con el objetivo de evaluar e informar a la Alta Gerencia acerca de la efectividad de las actividades realizadas.

6.6. Ejercicios y pruebas de los planes de continuidad del negocio

Las entidades deberán desarrollar un plan de ejercicios y pruebas a fin de verificar que las estrategias de continuidad definidas y los planes establecidos respaldan adecuadamente los objetivos de continuidad del negocio.

El plan deberá contener un cronograma anual formalizado, acorde a sus operaciones, procesos y estructura, que indique los escenarios contemplados, las fechas, áreas involucradas, procesos de negocio y sistemas alcanzados, entre otros aspectos. El cronograma deberá contemplar al menos uno de los escenarios de más alta criticidad.

En los ejercicios y pruebas de los planes de continuidad deberán participar, como mínimo, el responsable de la gestión de continuidad del negocio, las áreas de tecnología y seguridad de la información, las áreas usuarias relacionadas con los procesos de negocio, las terceras partes vinculadas y las áreas de auditoría interna.

Además, los resultados deberán permitir la evaluación de:

- La eficacia de las estrategias de continuidad adoptadas.
- El desempeño de las actividades de los participantes de acuerdo sus roles y responsabilidades.
- Los aspectos técnicos, logísticos y administrativos.
- El funcionamiento de la infraestructura de recuperación.
- La factibilidad de los procesos de reubicación del personal.
- Las deficiencias y oportunidades de mejora de los planes de continuidad.
- La efectividad de las estrategias de comunicación.

Se deberá mantener un registro detallado de los resultados de cada ejercicio, las observaciones y problemas detectados, y los planes de acción definidos para su corrección.

6.7. Mantenimiento de los planes de la continuidad del negocio

Las entidades deberán revisar y actualizar periódicamente los planes de continuidad del negocio y sus procedimientos vinculados a fin de asegurar su alineación con los objetivos del negocio, considerando, como mínimo:

- Cambios en las estrategias del negocio.
- La implementación de nuevos productos, servicios y/o infraestructuras tecnológicas.
- Cambios en los productos y servicios de terceras partes.
- Surgimiento de nuevos escenarios de amenazas.
- Cambios regulatorios.
- Indicadores clave de riesgo.
- Resultados de los ejercicios y pruebas realizadas.
- Resultados de las actividades de auditoría o evaluaciones internas o externas.

6.8. Control y reportes de gestión

Las entidades deberán definir un proceso de control sobre la gestión de la continuidad del negocio, mediante procedimientos, herramientas y métricas que permitan realizar un seguimiento y evaluación de las tareas desarrolladas y del cumplimiento de objetivos.

Las métricas deberán incluir indicadores o umbrales que permitan controlar los desvíos respecto de lo planificado, tanto para los planes de continuidad, los de capacitación como los de pruebas.

Entre las actividades de mejora continua, se deberán documentar, analizar e incluir las lecciones aprendidas de la ejecución de los planes, del análisis de impacto del negocio, la evaluación de riesgos y de los ejercicios y pruebas realizadas.

Se deberá establecer la frecuencia y los canales formales de comunicación de los resultados de la gestión de las áreas al Directorio y la Alta Gerencia. A su vez, la Alta Gerencia deberá informar sobre la gestión de la continuidad del negocio al Directorio o autoridad equivalente.

Sección 7. Infraestructura tecnológica y procesamiento

7.1. Gestión de la infraestructura tecnológica

Las entidades deberán definir estructuras, procesos y procedimientos para las actividades de gestión de actualizaciones y configuraciones, la implementación de cambios, el monitoreo de la infraestructura, la operación de los sistemas y la gestión de las comunicaciones. Los procesos establecidos deberán asegurar:

- La alineación de la infraestructura, las operaciones y las comunicaciones con la arquitectura empresarial y los objetivos de resiliencia.
- La preservación de la confidencialidad, integridad y disponibilidad de la información afectada.
- La implementación de medidas para evitar la existencia de puntos únicos de falla.
- La aplicación de mecanismos que permitan asegurar la trazabilidad de las actividades de gestión realizadas.
- Una gestión de incidentes alineada con lo dispuesto en la Sección 8.
- La alineación de los controles con lo establecido en la Sección 5.

Por otra parte, las entidades deberán establecer procesos para la gestión planificada y centralizada del registro y la respuesta de la demanda de servicios de tecnología que les permita:

- Capturar las solicitudes de actualización, ayuda, resolución de fallas, o algo similar.
- Establecer circuitos planificados para el tratamiento y la respuesta.
- Definir y comunicar los puntos de contacto.
- Realizar un seguimiento y mantener un registro de las solicitudes y las acciones tomadas.
- Identificar desvíos respecto de los circuitos planificados para el tratamiento y la respuesta.

7.2. Gestión de cambios

Las entidades deberán establecer un proceso que les permita registrar, evaluar, planificar, revisar, aprobar y comunicar los cambios en los activos de información antes de la implementación en entornos productivos. Los procedimientos que regulen el proceso de gestión de cambios deberán incluir:

- Una definición de roles y responsabilidades que mitigue los riesgos asociados a una inadecuada segregación de funciones.
- La implementación de controles por oposición de intereses acordes a los niveles de riesgo identificados.
- Controles para la separación de los entornos utilizados en las distintas etapas del ciclo de vida de desarrollo, adquisición y mantenimiento.
- La definición de criterios de aprobación y mecanismos de escalamiento alineados con el impacto de los cambios y los resultados de los análisis de riesgos.
- La ejecución de un análisis del impacto de los cambios sobre los activos de información involucrados.
- La implementación de controles que aseguren la separación del entorno de producción respecto del resto de los ambientes.
- La definición de procedimientos para la administración de servicios específicos (APIs, virtualización de hardware, etc.)

- La implementación de cambios en entornos productivos.
- El establecimiento de medidas que permitan revertir los cambios ante la detección de fallas o problemas asociados a su implementación.
- La aplicación de mecanismos que permitan asegurar la trazabilidad de las actividades realizadas y la integridad de los cambios que se implementan entre los distintos entornos.
- La definición de procedimientos específicos para el tratamiento, el control posterior y la identificación de las causas de los cambios de emergencia.

El proceso de gestión de cambios deberá estar en concordancia con lo dispuesto en la Sección 9: Desarrollo, adquisición y mantenimiento de software de este texto ordenado.

7.3. Actualización de la infraestructura tecnológica

En concordancia con los criterios establecidos para la gestión de cambios, las entidades deberán establecer un proceso de gestión de actualizaciones de infraestructura tecnológica, acorde con la arquitectura empresarial definida, que les permita:

- Desarrollar un plan de actualización de activos de información que considere las posibles vulnerabilidades por obsolescencia.
- Establecer un proceso para la implementación y el registro de los cambios, en concordancia con la gestión de activos de información.
- Evaluar los riesgos del uso de activos obsoletos e implementar efectivas medidas de mitigación.

Además, las entidades deberán implementar un proceso de gestión de las configuraciones que contemple los estándares de seguridad requeridos en la Sección 5. Este proceso deberá permitir:

- Establecer y actualizar los estándares de configuración para los componentes de hardware y software.
- Mantener información precisa y actualizada de las configuraciones del hardware y software que compone sus sistemas.
- Revisar y verificar las configuraciones de manera regular, monitorear los cambios no autorizados y los errores de configuración, y aplicar las adecuaciones correspondientes.
- Establecer mecanismos para verificar la integridad de software y detectar cambios no autorizados en las configuraciones.

Asimismo, se deberá establecer un proceso de gestión de actualizaciones de seguridad en línea con la gestión de amenazas y vulnerabilidades. Estas actualizaciones deberán ser probadas antes de su implementación en los entornos de producción para asegurar la compatibilidad con los sistemas existentes.

7.4. Gestión de las comunicaciones

Las entidades deberán establecer un proceso para la gestión de las comunicaciones que les permita:

- Una definición de roles y responsabilidades que mitigue los riesgos asociados a una inadecuada segregación de funciones.

- Mantener documentación detallada y actualizada del diseño de red, las interfaces, las conexiones y los elementos de seguridad.
- Asegurar la generación y la conservación de registros de actividades de los dispositivos de red.
- Establecer medidas para el monitoreo de las redes en tiempo real y el análisis del tráfico de red.
- Definir métricas para la detección de anomalías y la evaluación del nivel de calidad y disponibilidad de los servicios de red.
- Realizar revisiones periódicas de la infraestructura de comunicaciones, que les permitan identificar posibles debilidades.

7.5. Procesamiento de datos

Las entidades deberán establecer procesos de gestión para la planificación, ejecución, el monitoreo y el control de las operaciones de tecnología que permitan:

- Definir roles y responsabilidades que mitigue los riesgos asociados a una inadecuada segregación de funciones.
- Definir mecanismos que permitan asegurar la trazabilidad de la ejecución de los procesos.
- Implementar controles que aseguren que la eficiencia de sus operaciones se ajusta a las necesidades del negocio.
- Definir controles que permitan reanudar el procesamiento ante la detección de fallas o problemas en el flujo normal de ejecución.
- Asegurar que la totalidad de las actividades se encuentren documentadas.

Además, las entidades deberán establecer medidas para la detección, análisis, registro y corrección de errores y excepciones.

7.6. Gestión de copias de respaldo de datos

En concordancia con las estrategias de continuidad del negocio establecidas y el modelo de gestión de datos, las entidades deberán definir una estrategia para la realización de copias de respaldo que garantice la disponibilidad e integridad de los datos y los sistemas de información.

Adicionalmente, se deberá establecer un proceso para administrar el ciclo de vida de estas copias, que incluya:

- La definición de procedimientos para la realización, prueba y restauración de copias que indiquen, como mínimo: el alcance, la frecuencia, los tipos de medios, los períodos de retención y la cantidad de copias de seguridad.
- La aplicación de controles en la realización y conservación de copias que mitiguen los riesgos de modificación o eliminación de la información durante el período de retención.
- La implementación de controles de acceso, mecanismos de protección y cifrado para las copias de respaldo, de acuerdo con la clasificación de la información y la gestión de vulnerabilidades y amenazas.
- Medidas que brinden protección contra la replicación de malware y la corrupción de datos.
- La conservación de copias fuera de línea, en concordancia con la clasificación de datos e información.

En función de los requisitos legales y regulatorios, las entidades deberán establecer los plazos de conservación para las copias de respaldo históricas, y realizar al menos dos copias de la información de clientes, contable financiera y transaccional. Además, se deberán definir procedimientos y recursos que permitan la utilización de la información resguardada en cualquier momento de su ciclo de vida.

7.7. Monitoreo de la infraestructura tecnológica y procesamiento

Las entidades deberán implementar procesos de monitoreo de la infraestructura tecnológica y del procesamiento de las operaciones para prevenir, detectar y responder oportunamente ante eventos no deseados, así como obtener información sobre el rendimiento de las capacidades y funcionamiento.

Se deberán establecer indicadores que permitan medir el desempeño de la infraestructura tecnológica y el procesamiento, tanto de los servicios internos, como de los provistos por terceras partes.

Se deberán considerar, al menos:

- Utilización de los recursos y disponibilidad de los servicios propios y de terceros.
- Tiempo de respuesta o tiempo medio de conexión por servicio.
- Fallos de los sistemas.
- Eficiencia del procesamiento de transacciones.
- Métricas de gestión de cambios y actualizaciones.
- Métricas de la gestión de servicios de tecnología.

Los resultados del monitoreo de la infraestructura y el procesamiento deberán ser considerados para la mejora continua y la planificación de las actualizaciones de acuerdo con la arquitectura empresarial. Asimismo, se deberán reportar periódicamente a la Alta Gerencia los resultados de la gestión del monitoreo.

Sección 8: Gestión de ciberincidentes

En concordancia con los textos ordenados sobre “Lineamientos de respuesta y recuperación ante ciberincidentes” y “Protección de usuarios de Servicios Financieros” las entidades deberán establecer un marco de gestión de ciberincidentes que contemple medidas técnicas y organizativas que les permitan minimizar impactos y contener su propagación mediante la aplicación de controles para la respuesta y recuperación.

El marco de gestión deberá estar alineado con:

- Los objetivos estratégicos del negocio.
- La gestión de riesgos de tecnología y seguridad de la información.
- El marco de gestión de seguridad de la información.
- El marco de gestión de la continuidad del negocio.
- Los procesos de gestión de la infraestructura tecnológica.
- Los procesos críticos de la entidad y los asociados a las normas de protección del usuario de servicios financiero.

Las políticas para la gestión de ciberincidentes deberán definir, al menos:

- El alcance y las áreas participantes de la respuesta ante ciberincidentes para la entidad, indicando los roles y responsabilidades de cada área.
- Los objetivos y prioridades de la respuesta alineados a la gestión del riesgo y la continuidad del negocio.
- Los principios para priorizar y escalar ciberincidentes.
- Las métricas para realizar los controles para una gestión efectiva.

8.1. Preparación de la respuesta ante ciberincidentes

Las entidades deberán establecer normas y procedimientos que permitan gestionar, controlar y documentar las actividades de la gestión de ciberincidentes; contener el impacto y restablecer capacidades y servicios, y prevenir nuevos incidentes e investigar causas.

Las normas y procedimientos deberán contener, como mínimo:

- Los circuitos y flujos de actividades a seguir por la entidad ante los ciberincidentes, y los criterios de priorización y escalamiento.
- La definición de una taxonomía que contenga la identificación y descripción de los ciberincidentes considerados por la entidad.
- La descripción de las responsabilidades de las áreas participantes en la respuesta a ciberincidentes, incluyendo la evaluación de los aspectos legales, la coordinación de la comunicación interna y externa, y la investigación de la causa raíz.
- Criterios para la priorización de la atención de ciberincidentes basados en la criticidad o impacto para el negocio, los servicios, los procesos o las personas afectadas.
- La alineación de las actividades con la política de continuidad del negocio cuando corresponda.
- Criterios para el análisis e investigación forense y para la conservación de evidencia.
- Circuitos de comunicación internos y externos.
- De acuerdo con la evaluación de riesgo, definiciones referidas a la conservación de evidencias para la investigación posterior en cumplimiento de prácticas forenses adoptadas.

8.1.1. Registro y repositorio de ciberincidentes

Las entidades deberán establecer y mantener un registro completo de sus ciberincidentes que permita la identificación, la trazabilidad y la evidencia de las acciones tomadas hasta su cierre.

Para ello, se deberá establecer un repositorio para el registro del ciberincidente y las evidencias que permita asegurar su integridad, trazabilidad, disponibilidad y confidencialidad.

Además, las entidades deberán realizar un registro del seguimiento de las actividades hasta la identificación de la causa raíz de los ciberincidentes a fin de asegurar su resolución y evitar su recurrencia. Cuando el origen no se encuentre bajo control de la entidad, también deberá dejarse evidencia de las acciones tomadas para gestionar su seguimiento.

Se deberá analizar la información registrada con el objetivo de detectar la correlación entre ellos para prevenir nuevos ciberincidentes o para la investigación de las causas raíz.

Cuando los ciberincidentes se relacionen o surjan de reclamos de clientes o posibles fraudes, se deberán vincular los respectivos registros con el objetivo de realizar un seguimiento conjunto e identificar todas las acciones ejecutadas.

8.1.2. Investigación de ciberincidentes

Los procedimientos relacionados con la investigación de ciberincidentes deberán permitir:

- Identificar aquellos incidentes que requerirán el resguardo de evidencia para investigación posterior.
- El resguardo de la evidencia para investigación por parte de las autoridades en línea con las buenas prácticas en materia forense informática.

8.1.3. Comunicación y notificación de los ciberincidentes

Los procedimientos de comunicación y notificación deberán permitir la comunicación eficaz de los ciberincidentes para que la respuesta sea oportuna y planificada. Las entidades deberán definir:

- Roles para la atención ante distintos incidentes o escenarios.
- Mecanismos para la comunicación con terceras partes, para la gestión y el reporte de ciberincidentes a las autoridades.
- Un punto de contacto para reportar ciberincidentes para los empleados, terceras partes y público en general, a fin de mitigar el impacto de manera oportuna.

8.2. Ejercicios y pruebas de la respuesta ante ciberincidentes

Las entidades deberán establecer un plan de pruebas de las actividades previstas para la respuesta ante ciberincidentes que incluya, al menos, la periodicidad, los objetivos y el alcance de la prueba.

Se deberán definir distintos tipos de prueba que permitan evaluar las capacidades técnicas, y la coordinación y comunicación oportuna entre las áreas. Se deberán documentar los resultados e incorporar las lecciones aprendidas en los planes y procedimientos correspondientes.

8.3. Control y reportes de gestión

Las entidades deberán definir un proceso de control sobre la gestión de ciberincidentes, mediante procedimientos, herramientas y métricas que permitan realizar un seguimiento y evaluación de las tareas desarrolladas, y la identificación de oportunidades de mejora.

Las métricas deberán incluir indicadores o umbrales que permitan controlar los desvíos respecto de lo planificado y establecer planes de acciones correctivas cuando sea necesario. Adicionalmente, se deberán evaluar los resultados de las actividades de mejora continua.

De acuerdo con sus operaciones, procesos y estructura, las entidades deberán promover la implementación de indicadores automatizados, como así también la generación de alertas ante desvíos respecto de los umbrales.

Además, se deberá establecer la frecuencia y los canales formales de comunicación de los resultados de la gestión de las áreas al Directorio y la Alta Gerencia.

Sección 9: Desarrollo, adquisición y mantenimiento de “software”

9.1. Requisitos para los sistemas y aplicaciones

Las entidades deberán diseñar e implementar sistemas de información que les permitan registrar y procesar la totalidad de sus operaciones de negocio. Los sistemas y aplicaciones deberán incluir controles automatizados que:

- Aseguren la integridad y confiabilidad en el ingreso, el procesamiento, la actualización y la consolidación de la información.
- Limiten la modificación y la eliminación de datos de las operaciones concretadas, movimientos y saldos.
- Aseguren la consistencia entre los saldos operativos y contables.
- Permitan la administración de los parámetros que limiten el ingreso de datos.
- Brinden una adecuada integración entre los sistemas que procesan la información de la entidad.

Se deberán implementar controles para la identificación única del cliente y el registro de los datos obligatorios de acuerdo con las normas vigentes. Además, deberán realizarse procesos periódicos de control y depuración.

En todos los sistemas y aplicaciones, se deberán implementar esquemas de autorización acordes a la política de control de accesos para el ingreso, modificación y baja de operaciones y parámetros.

Se deberá implementar funcionalidad para la gestión de usuarios y perfiles, y la asignación de permisos sobre las funciones del sistema. Además, se deberán definir funciones que permitan ejercer un control sobre la asignación de perfiles de acuerdo con los roles y funciones establecidos en la entidad.

Todos los sistemas deberán generar registros de auditoría que permitan asegurar la trazabilidad de cada una de las acciones realizadas y contengan, al menos:

- Una identificación univoca.
- El tipo de evento o acción realizada.
- La fecha y hora.
- La identificación de los usuarios intervinientes.
- La identificación del dispositivo, la aplicación o canal de origen.
- En caso de modificación de parámetros, el valor anterior y posterior a la actualización.

Se deberán establecer controles para el resguardo de la integridad, disponibilidad y confidencialidad de todos los registros de auditoría.

La información que da soporte a los registros contables y los registros de auditoría deberán ser conservados en condiciones de ser recuperados por un término no menor a seis (6) años. Además, deberán estar disponibles de manera inmediata en caso de que la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias los requiera.

Las entidades deberán contar con documentación funcional, técnica y de usuario actualizada de sus sistemas de información, que considere aspectos tales como:

- Diagrama del sistema y de los programas que lo componen.
- Descripción del "hardware" y "software", y lenguaje de programación utilizado.

- Interfaces con otros sistemas.
- Su interrelación con las redes de telecomunicaciones.
- Descripción de las principales funciones y opciones del sistema.
- Guías de usuario sobre las funcionalidades del sistema, procedimientos y salidas.

9.1.1. Requisitos para la generación de los regímenes informativos

Las entidades deberán contar con sistemas o procesos automatizados para la generación de los regímenes informativos requeridos por el Banco Central de la República Argentina.

Además, se deberán implementar controles que limiten la intervención manual de los usuarios en el proceso y la realización de ajustes a la información generada en forma automática.

Cuando haya información que debe ser ingresada manualmente, se deberán implementar:

- Programas específicos con un adecuado esquema de autorizaciones.
- Controles sobre los valores ingresados.
- Restricciones que impidan la alteración de la información generada automáticamente.
- Trazabilidad completa de las operaciones.

9.2. Gestión del ciclo de vida de “software”

Las entidades deberán establecer un marco para la gestión del ciclo de vida de desarrollo, adquisición y mantenimiento de software que contemple:

- Objetivos estratégicos del negocio.
- La arquitectura empresarial.
- La evaluación de los riesgos y la implementación de controles de mitigación de acuerdo con lineamientos establecidos dentro de la sección 3. Gestión de riesgos de tecnología y seguridad de la información.
- Las metodologías de gestión de proyectos establecidas y los aspectos aplicables de la Sección 4. Gestión de Tecnología de la Información.
- Los aspectos aplicables de la Sección 5. Gestión de seguridad de la información.
- Los requerimientos de gestión de cambios definidos en la Sección 7. Infraestructura tecnológica y procesamiento.

Este marco de gestión deberá establecer como mínimo:

- La asignación de roles y responsabilidades.
- La documentación que describa las metodologías a utilizar en el ciclo de vida del software.
- Criterios para la evaluación de requerimientos.
- Procedimientos para la evaluación y selección de proveedores.
- Procedimientos de evaluación para la incorporación o integración de componentes de terceras partes en el ciclo de vida del software. Esto incluye código abierto, API y algoritmos de inteligencia artificial o aprendizaje automático.
- Criterios para la construcción y el uso de modelos de inteligencia artificial, los procesos de recolección y preparación de datos de entrenamiento, las actividades de verificación y validación de las respuestas.

- Estándares que establezcan buenas prácticas para el desarrollo y mantenimiento de software.
- Controles para asegurar la disponibilidad y actualización de los programas fuentes, y la documentación técnica y funcional.
- Procedimientos para la implementación del modelado de amenazas.
- Procedimientos que establezcan los criterios para la realización de pruebas de software y para la revisión de código.
- Planes de capacitación y concientización acordes a los roles y responsabilidades definidos.
- Procedimientos para las evaluaciones de seguridad en la adquisición de software y en la incorporación de componentes de software de terceras partes a los desarrollos propios.
- Procedimientos que establezcan criterios para la calidad de software y su aseguramiento.

9.2.1. Análisis de requerimientos, diseño y codificación

Dentro el marco de gestión del ciclo de vida de desarrollo, adquisición y mantenimiento de software, se deberán identificar, definir y documentar los requisitos funcionales, regulatorios y de seguridad del software.

Adicionalmente, se deberán documentar los resultados de las evaluaciones de seguridad y funcionalidad realizadas, en especial:

- Cuando se integren al ciclo de vida componentes de software desarrollados por terceras partes.
- Cuando los sistemas o aplicaciones integren servicios que permitan el intercambio de datos con terceras partes.

Las entidades deberán ajustarse a las normas y procedimientos definidos para el desarrollo seguro y modelado de amenazas. Además, cada proyecto deberá contar con la documentación establecida en la metodología utilizada. Se deberán definir mecanismos para verificar la integridad del software durante todo el ciclo de vida.

9.2.2. Pruebas, implementación y mantenimiento

Las entidades deberán establecer y ejecutar planes de prueba del software o de los componentes que sean acordes a los resultados de los análisis de riesgos y permitan:

- Determinar y documentar el alcance en función de los riesgos identificados.
- Combinar diferentes enfoques de pruebas automáticas y manuales.
- Determinar los riesgos vinculados con los procesos de pruebas y la dificultad para documentar y predecir las respuestas de la IA, que justifican la necesidad de un monitoreo continuo con métricas establecidas previamente en la etapa de operación del sistema (post implementación).
- Documentar el diseño, creación y preparación de datos de prueba que consideren la protección de datos personales o sensibles.
- Revisar y actualizar periódicamente las reglas de validación y prueba del software.
- Realizar y documentar pruebas específicas antes de la implementación de cambios o nuevas versiones de software propio y de terceras partes.
- Evaluar y aceptar los resultados de las pruebas antes de la implementación de los cambios en los entornos de producción.

- Comunicar los resultados de las pruebas para contribuir con la mejora continua.

Por otra parte, las entidades deberán contar con pruebas de vulnerabilidades realizadas por terceros independientes sobre las aplicaciones que manejen datos de clientes, transaccionales o financieros.

Se deberán documentar los hallazgos detectados en la revisión del código fuente y en las pruebas de seguridad. Además, se deberán registrar y evaluar los riesgos, y establecer medidas para su tratamiento y aceptación.

Para la implementación del software en los entornos productivos se deberán considerar los requisitos establecidos para la gestión de cambios y se deberán establecer controles que aseguren la integridad y trazabilidad de las versiones de código de software.

Las entidades deberán establecer procedimientos para el mantenimiento y control de los sistemas y aplicaciones que consideren:

- Evaluación y actualización de componentes obsoletos propios y de terceras partes.
- Cambios en los servicios de terceras partes consumidos por los sistemas de la entidad.
- Los resultados de la gestión de vulnerabilidades.
- La evolución de los sistemas y aplicaciones que utilizan algoritmos de inteligencia artificial y aprendizaje automático.

9.2.3. Aseguramiento de la calidad

Las entidades deberán definir un proceso con el objetivo de que el software cumpla con los estándares de calidad y seguridad, las buenas prácticas, y el marco legal y normativo. Los roles y responsabilidades relativos al aseguramiento de la calidad deberán ser independientes de las áreas de desarrollo y prueba.

Este proceso deberá incluir, como mínimo, normas y procedimientos vinculados con la revisión e inspección de:

- El cumplimiento de los procedimientos y la aplicación de las metodologías definidas.
- La ejecución de los planes de prueba definidos.
- La capacitación de los integrantes de los equipos en función de las herramientas, tecnologías y de aspectos de seguridad.

Además, se deberán establecer métricas e indicadores que permitan evaluar la gestión del software y las actividades de seguimiento respecto de los umbrales definidos.

Las entidades deberán considerar los resultados del proceso de aseguramiento de la calidad para la mejora continua del marco de gestión del ciclo de vida de desarrollo, adquisición y mantenimiento de software.

Sección 10. Gestión de la relación con terceras partes

Las entidades podrán delegar en terceras partes procesos, servicios y/o actividades vinculadas con los procesos de tecnología y seguridad de la información, de acuerdo con las disposiciones de la sección 2 del Texto Ordenado “Expansión de entidades financieras”.

No se encuentran alcanzados por los requisitos de esta sección:

- Los servicios que brindan información de manera general sobre los mercados financieros.
- Los servicios de adopción obligatoria por regulación del sistema financiero.
- Los servicios brindados por organismos del Estado.
- Las actividades de corresponsalía bancaria.
- Los servicios de procesamiento de pago con tarjetas de crédito.

No se podrán delegar procesos, servicios y/o actividades con terceras partes que desempeñen funciones de auditoría interna y/o externa en la entidad.

Las delegaciones de procesos, servicios o actividades en terceras partes no implican la transferencia de las responsabilidades primarias enunciadas en la presente normativa.

En función de sus operaciones, procesos y estructura, las entidades deberán considerar el establecimiento de un sector o una función responsable de la gestión de la relación con las terceras partes.

Previo al inicio de la relación, las entidades deberán informar las características del proceso, servicio y/o actividad a delegar a la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

10.1. Marco de gestión de la relación con terceras partes

Las entidades deberán establecer una política y un marco para la gestión de procesos, servicios y/o actividades delegadas en terceras partes que considere:

- La definición de roles y responsabilidades para las distintas actividades de la gestión.
- Las medidas de seguridad de acuerdo con los resultados de la gestión de riesgos de tecnología y seguridad; y los riesgos propios de la delegación.
- Procedimientos para la selección y contratación de terceras partes.
- La identificación y documentación de los servicios y actividades delegadas.
- La identificación de los puntos de contacto para los aspectos legales y los relacionados con tecnología, seguridad de la información y gestión de ciberincidentes.
- La elaboración y mantenimiento de un catálogo con la información de los servicios y actividades delegadas en terceras partes.
- La continuidad de los servicios de acuerdo con los resultados de los análisis de riesgos.
- Mecanismos para la gestión de los conflictos de intereses.
- Mecanismos para la gestión de ciberincidentes.
- La elaboración de procedimientos para la supervisión del cumplimiento de los acuerdos formalizados.
- La implementación de auditorías independientes sobre los servicios y actividades gestionados por terceras partes que permitan evaluar la gestión de riesgos y la alineación con los procesos de tecnología y seguridad de la información de la entidad.

Por otra parte, las entidades deberán evaluar posibles escenarios de finalización planificada o forzada de los procesos, servicios o actividades provistos por terceras partes, y establecer planes de finalización que les permitan mitigar los riesgos de interrupción, incumplimiento de los requisitos legales y regulatorios, o degradación de la calidad. Los planes de finalización deberán considerar la obtención de los datos, los programas fuentes, y la documentación de los sistemas y aplicaciones.

10.2. Formalización de la relación

Las entidades deberán formalizar en todos los casos las relaciones con terceras partes que brinden procesos, servicios y/o actividades delegadas de acuerdo con los procedimientos establecidos. Se deberán fijar como mínimo:

- La naturaleza, el alcance de los procesos, servicios y/o actividades a delegar y las responsabilidades de las partes.
- La duración de la contratación o delegación y cláusulas específicas que regulen la renovación automática.
- Los niveles mínimos de prestación y métricas de desempeño.
- La existencia de planes de continuidad.
- Los derechos a realizar auditorías por parte de la entidad.
- Los mecanismos de comunicación sobre los cambios que puedan afectar las condiciones en la prestación del servicio.
- Los acuerdos sobre confidencialidad.
- Los mecanismos para la resolución de disputas.
- Los procedimientos coordinados para la gestión de ciberincidentes.
- El cumplimiento del marco legal y regulatorio aplicables.
- Disposiciones que permitan el acceso irrestricto por parte de la Superintendencia de Entidades Financieras y Cambiarias a las instalaciones, áreas de control y la documentación relacionada.
- Los mecanismos de notificación sobre cambios en el control accionario y en los cambios de niveles gerenciales de las terceras partes.
- Las responsabilidades en los circuitos de reclamos de clientes o usuarios de servicios financieros de la entidad.
- Procedimientos y protocolos de comunicación que permitan el cumplimiento efectivo de los controles sobre los procesos, servicios y actividades delegadas.
- La designación formal de un responsable en representación de la tercera parte para el tratamiento de aspectos vinculados con la delegación, de acuerdo con las características del servicio y los resultados de los análisis de riesgo.
- Los mecanismos para la eliminación de los datos de la entidad gestionados por terceras partes, una vez extinguida la relación.
- Los procedimientos para la finalización de los servicios de acuerdo con la evaluación de riesgos.

Los documentos que instrumenten la contratación o delegación deberán contener disposiciones que aseguren que los procesos, servicios y actividades delegadas en terceras partes cumplan con los requisitos exigidos en la presente norma, de acuerdo con su evaluación de riesgos.

Los servicios de mensajería financiera de SWIFT y EUROCLEAR serán evaluados teniendo en cuenta sus condiciones particulares de contratación.

10.2.1. Subcontrataciones de las terceras partes

Los documentos que instrumenten la contratación o delegación con terceras partes deberán establecer formalmente la responsabilidad del prestador primario respecto de:

- Todos los procesos, servicios y/o actividades prestadas por sí mismo o por medio de subcontratistas, con independencia de la ubicación geográfica.
- La notificación a la entidad de todas las subcontrataciones con la identificación de los servicios y actividades involucrados.

Además, todos los subcontratistas deberán asumir formalmente:

- La responsabilidad de cumplir con el marco legal y regulatorio aplicable.
- La asignación de derechos de acceso y auditoría, tanto para la entidad, como a la Superintendencia de Entidades Financieras y Cambiarias.

10.3. Control y monitoreo

Las entidades deberán definir un proceso de control que les permita realizar un seguimiento y evaluación de los procesos, servicios y actividades de tecnología y seguridad de la información delegados en terceras partes.

Deberán existir procedimientos para la ejecución de controles sobre las terceras partes, la evaluación del cumplimiento de los requisitos regulatorios y los niveles de servicio acordados, y el seguimiento de las solicitudes de adecuación, en caso de incumplimientos.

La periodicidad de las actividades de control y monitoreo deberá definirse de acuerdo con el nivel de riesgo y la criticidad de los procesos, servicios o actividades delegados.

10.3.1. Informes de terceros independientes

Los informes de las evaluaciones realizadas por terceros independientes sobre los procesos, servicios y actividades delegadas en terceras partes serán considerados complementarios a las actividades de control y monitoreo de la entidad, siempre que:

Estén elaborados de acuerdo con procesos aceptados internacionalmente.

Los alcances y los resultados permitan verificar los controles implementados.

Se realicen auditorías o actividades de revisión adicionales cuando el alcance no cubra la totalidad de los requisitos normativos y los riesgos identificados.

10.4. Informes de auditoría interna y externa

Se deberán realizar auditorías internas sobre los procesos, servicios y actividades delegadas en terceras partes que incluyan revisiones del cumplimiento de los requisitos legales y regulatorios. Los informes deberán ser remitidos a la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

La periodicidad de los informes de auditoría deberá definirse de acuerdo con el nivel de riesgo y la criticidad de los servicios o actividades delegados.

Adicionalmente, se deberán remitir a la Gerencia de Auditoría Externa de Sistemas los informes de los auditores externos efectuados con motivo de sus revisiones sobre los servicios y actividades delegados en terceras partes.

Sección 11: Canales Electrónicos

11.1. 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 11.6.:

11.1.1. Cajeros Automáticos (ATM).

11.1.2. Terminales de Autoservicio (TAS).

11.1.3. Banca Móvil (BM).

11.1.4. Banca Telefónica (BT).

11.1.5. Banca por Internet (BI).

11.1.6. Puntos de Venta (POS).

11.1.7. Plataforma de Pagos Móviles (PPM).

11.2. 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. Por otra parte, deben informar a la Gerencia de Auditoría Externa de Sistemas la estructura e interrelaciones orgánicas y operativas que en sus organizaciones se corresponda:

11.2.1. 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.

11.2.2. 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.

11.2.3. Integridad y Registro (IR)

Proceso 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 Canales Electrónicos y las técnicas que brinden trazabilidad y permitan su verificación. Incluye, pero no se limita a transacciones, registros de auditoría y esquemas de validación.

11.2.4. Monitoreo y Control (MC)

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

11.2.5. Gestión de Incidentes (GI)

Proceso relacionado con el tratamiento de los eventos y consecuentes incidentes de seguridad en Canales Electrónicos, su detección, evaluación, contención y respuesta, así como las actividades de escalamiento y corrección del entorno técnico y operativo.

11.3. 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 sus Canales Electrónicos.

11.3.1. De la Matriz de Escenarios y la Gestión de Riesgo Operacional de Tecnología

11.3.1.1. Deben encuadrar la operatoria de los Canales Electrónicos que gestionen, dentro de los escenarios comprendidos en la Matriz de Escenarios del punto 11.5., implementando cómo mínimo y según la criticidad que se establezca, los requisitos indicados para cada escenario aplicable.

11.3.1.2. Atento a las normas sobre “Lineamientos para la Gestión de Riesgos en las Entidades Financieras”, las entidades 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 este Banco Central para cada escenario o cuando no esté indicado, por lo establecido en el punto 11.4.2.

11.3.1.3. Lo indicado en el punto 11.3.1.2., debe encontrarse documentado y formar parte de la metodología de gestión de riesgos operacionales 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.

11.3.1.4. 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

11.3.2. Del cumplimiento de los requisitos técnico-operativos mínimos

11.3.2.1. 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 11.7. y subsiguientes.

11.3.2.2. 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:

11.3.2.2.1. Concientización y Capacitación. Complementariamente a lo indicado en el punto 11.2.1., 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.

11.3.2.2.2. Control de Acceso. Complementariamente a lo previsto en el punto 11.2.2., 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.

11.3.2.2.3. Integridad y Registro. Complementariamente a lo indicado en el punto 11.2.3., 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.

11.3.2.2.4. Monitoreo y Control. Complementariamente a lo previsto en el punto 11.2.4. las entidades deben contar con recursos técnicos y humanos dispuestos para asegurar un control permanente y continuo de todos sus Canales Electrónicos y una clasificación de los eventos registrables, así como patrones de búsqueda y correlación.

11.3.2.2.5. Gestión de Incidentes. Complementariamente a lo indicado en el punto 11.2.5., las entidades deben arbitrar los esfuerzos necesarios para contar en sus organizaciones o a través de terceros bajo coordinación y control propio, con equipos de trabajo especializado en la atención, diagnóstico, análisis, contención, resolución, escalamiento e informe de los incidentes de seguridad de todos sus Canales Electrónicos, de manera formal e integrada.

11.3.3. De la responsabilidad sobre los Canales Electrónicos

11.3.3.1. El Directorio o autoridad equivalente de la entidad, es el responsable primario de la gestión de seguridad informática de la operatoria de los Canales Electrónicos desde el primer momento en que sus clientes se suscriben a los servicios ofrecidos por su intermedio o reciben medios de pago emitidos por ellas o en su nombre para su uso dentro de los alcances establecidos en el acuerdo de prestación.

11.3.3.2. La responsabilidad de las entidades financieras en los servicios y operaciones cursadas por medio de Canales Electrónicos 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. Excluye aquellos medios físicos o lógicos propiedad y tenencia exclusiva de los clientes, siempre que admitan limitar su uso y disponibilidad a la compatibilidad con los mecanismos necesarios para brindar un servicio financiero seguro.

11.3.3.3. Las empresas prestadoras de servicios de procesamiento, transporte, custodia y/o tareas o procesos de seguridad informática relacionados con los Canales Electrónicos 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, se encuentran alcanzadas por las condiciones establecidas en la Sección 2. de las normas sobre “Expansión de entidades financieras” y en otras regulaciones técnicas complementarias.

11.3.3.4. Las entidades financieras deben establecer e informar a este Banco Central la estructura orgánica dispuesta y la nómina de responsables de las tareas relacionadas con los Procesos de Referencia indicados en el punto 11.2. e informar de cualquier novedad o cambio efectuado a la misma 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 dónde se encuentre descentralizada parte o la totalidad de los servicios de Canales Electrónicos.

11.3.3.5. 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.

11.4. Escenarios de Canales Electrónicos

11.4.1. 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.

11.4.2. 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 11.4.1. 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 11.7).
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 11.7).
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 o el sistema financieros 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 podrá 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.

11.5. 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 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.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Matriz de Escenarios (continuación)					
Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
	ETR007	Solicitud, formalización y acreditación de operaciones de crédito. Para créditos preaprobados aplica RMC012 con criticidad 1.	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; RMC012; 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.

11.6. 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 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 financieras, 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 necesarias 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 financiero 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 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 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 cambiarias y/o financieras, de instrucción legal por medio financiero o pago de bienes y servicios.

Sesión en Canales Electrónicos. Comprende al período durante el cual un consumidor (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, 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.

11.7. Tablas de requisitos técnico-operativos

11.7.1. 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.	
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.	

11.7.2. 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 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, 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 11.5. b. DES para dispositivos que permitan transacciones establecidas con criticidad de nivel distinto a 1 en los escenarios del punto 11.5.	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 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).	
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.	

Tabla de requisitos de Control de Acceso		
Código de requisito	**Descripción de requisito**	**Alcance**
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. 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. 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.
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.	

Tabla de requisitos de Control de Acceso		
Código de requisito	**Descripción de requisito**	**Alcance**
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 modifique los valores generados en su primera presentación ante el CE. 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 financiero 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 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 de la clave personal (PIN) asociado a una tarjeta TD/TC basada exclusivamente en banda magnética, según el RCA044 punto a. debe garantizar al menos una de las siguientes condiciones: a. Dos claves personales (PIN), una para el uso del canal ATM y otra para los canales POS e implementaciones PPM basadas en lectores para teléfonos celulares (dongle), con valores distintos entre sí. b. Una clave personal (PIN) única para todos los canales y la devolución inmediata de los montos involucrados en caso de desconocimiento por parte del cliente de una transacción efectuada en estas condiciones. c. Una clave personal (PIN) exclusiva para el canal ATM y la devolución inmediata de los montos involucrados en caso de desconocimiento por parte del cliente de una transacción efectuada en estas condiciones en los canales POS y PPM.	
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.	

Tabla de requisitos de Control de Acceso		
Código de requisito	**Descripción de requisito**	**Alcance**
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 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 financiera 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.
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. 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. 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.	

Tabla de requisitos de Control de Acceso		
Código de requisito	**Descripción de requisito**	**Alcance**
	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 financieros y/o servicios de un tercero que permitan el acceso y ejecución de transacciones consideradas en los escenarios del punto 11.5. 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 o, en el caso de elementos de autenticación dinámica (tokens, tarjetas de coordenadas, entre otros). b. Descartarse en el caso de TD/TC.	
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 11.5. 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		
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 11.5. 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 11.5. 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 11.5. 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.	

11.7.3. 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 las 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.	
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:	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de requisitos de Integridad y Registro		
Código de requisito	**Descripción de requisito**	**Alcance**
	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, 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 financiero (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.	
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, 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. 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.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de requisitos de Integridad y Registro		
Código de requisito	**Descripción de requisito**	**Alcance**
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 sigla 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.	

11.7.4. 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, 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.	
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.	

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Tabla de Requisitos de Monitoreo y Control		
Código de requisito	**Descripción de requisito**	**Alcance**
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.	
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.	

11.7.5. 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.	

Sección 12. Glosario de términos

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

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

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

Anomalía: Evento, comportamiento o funcionamiento no esperado.

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

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

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

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

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

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

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

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

Ciberincidente o Incidente de tecnología y seguridad. Evento cibernético que:

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

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

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

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

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

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

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

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

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

Dato: Pieza de información.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Gestión del portafolio: Gestión coordinada del conjunto de los proyectos para lograr objetivos específicos de negocio.

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

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

Integridad: Cualidad de exacto y completo.

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

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

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

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

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

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

Práctica: Actividad realizada de manera recurrente.

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

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

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

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

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

Seguridad de la información: La preservación de la integridad, disponibilidad y confidencialidad de la información. Además, podría incluir la autenticidad, la trazabilidad, la rendición de cuentas, el no repudio y la confiabilidad.

Shadow IT: Se refiere a software, hardware, servicios y dispositivos no autorizados por la organización que operan en el entorno de TI.

Subcontratación: Práctica en virtud de la cual una tercera parte encarga a un subcontratista parte de lo que se le ha encomendado.

Tercera parte: Quien brinda procesos, servicios y/o actividades que han sido formalmente delegados por la entidad de acuerdo con lo establecido en la Sección 2 del Texto Ordenado “Expansión de entidades financieras”. Se considera dentro de esta definición a una entidad perteneciente a un grupo corporativo (global o doméstico) o una entidad externa al grupo corporativo, con la cual se ha establecido un contrato para la realización de procesos, servicios y/o actividades.

Tolerancia al riesgo: Nivel aceptable de variación respecto del apetito de riesgo definido en el logro de los objetivos de la entidad.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas.