BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

REQUISITOS MÍNIMOS PARA LA GESTIÓN Y CONTROL DE LOS RIESGOS DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

-Última comunicación incorporada: "A" 8401-

Texto ordenado al 13/02/2026

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”

-Índice-

-Índice-

1.1. Sujetos obligados

1.1.1. Entidades financieras.

1.1.2. Infraestructuras del Mercado Financiero conocidas como Sistemas de Pago de importancia sistémica: INTERBANKING, COELSA, LINK y NEWPAY.

1.1.3. Proveedores de servicios de pago (PSP) incluidos en el Registro de PSP del Banco Central de la República Argentina (BCRA).

1.2. Aspectos generales

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

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

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

Adicionalmente las entidades deberán promover:

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

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 las normas sobre “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.

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.

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 por 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.

Cuando no sea posible delimitar las funciones involucradas en alguno de los proyectos, se deberán considerar las exigencias establecidas en la Sección 2 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.

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.

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 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.

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 con 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.

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.

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.

En concordancia con las normas 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.

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 (SEFyC) 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 (BCRA).

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.
- Las metodologías de gestión de proyectos establecidas y los aspectos aplicables de la Sección 4.
- Los aspectos aplicables de la Sección 5.
- Los requerimientos de gestión de cambios definidos en la Sección 7.

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.

Las entidades podrán tercerizar procesos, servicios y/o actividades vinculados con los procesos de tecnología y seguridad de la información, dentro del país como en el exterior.

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 tercerizar procesos, servicios y/o actividades en terceras partes que realicen funciones de auditoría interna y/o externa.

Las entidades que tercericen procesos, servicios y/o actividades vinculados a la tecnología y seguridad de la información no estarán liberadas de sus responsabilidades, presentes o futuras, que les correspondan conforme a las disposiciones legales y reglamentarias y a las normas dictadas por el BCRA.

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.

La contratación o tercerización deberá contener disposiciones que aseguren que los procesos, servicios y actividades tercerizados cumplan con los requisitos exigidos en estas normas, de acuerdo con su evaluación de riesgos. La evaluación de los riesgos de todos los prestadores de servicio deberá estar documentada y aprobada por las máximas autoridades locales de la entidad.

10.1. Exigencia de notificación previa.

Las entidades deberán informar a la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias (SEFYC) las características de los servicios críticos a tercerizar**,** con una antelación no inferior a 60 días corridos del inicio de la tercerización.

La notificación previa de los servicios críticos a tercerizar deberá contener:

- La naturaleza de los servicios, conforme a la siguiente taxonomía:

  - Procesamiento de datos en infraestructuras tradicionales.
  - Infraestructura y procesamiento en modalidad *Infrastructure as a Service* (IaaS).
  - Soluciones en modalidad *Platform as a Service* (PaaS).
  - Soluciones en modalidad *Software as a Service* (SaaS).
  - Administración y gestión de datos.
  - Control de acceso a la infraestructura, a los sistemas y a los datos.
  - Operaciones de seguridad (incluye SOC).
  - Gestión de ciberincidentes (en cualquiera de sus etapas).

- Actividades de *back-office* con soporte tecnológico.
- Administración de pagos.
- Gestión de las comunicaciones y redes.
- Desarrollo, soporte y mantenimiento.
- Gestión de copias de respaldo.
- Otros servicios considerados críticos.

- Una descripción de los servicios y actividades alcanzados.

- Las ubicaciones geográficas (país, región, ciudad) donde se desarrollarán cada una de las actividades.

- Las ubicaciones geográficas (país, región, ciudad) donde se realizarán las tareas de control sobre las actividades.

- La fecha de puesta en funcionamiento de las actividades.

- Los datos del responsable de contacto directo en el tercero prestador de servicios (nombre, función, teléfono y correo electrónico).

- Cuando la actividad contemple subcontrataciones (“n-ésimas partes”), deberá identificarse cada uno de los prestadores, la actividad que realizará y las ubicaciones geográficas.

- Los instrumentos que formalicen la tercerización.

- Un plan de continuidad operativa que cumpla con los requisitos normativos vigentes.

- Contar con soluciones de continuidad alternativas conforme a lo previsto en las Secciones 3. y 6.

- En el caso de tercerización de servicios intra-grupo en el exterior, se deberá contar con una certificación escrita del ente supervisor del país de origen que indique que:

  - Se encuentra en conocimiento y no objeta la tercerización.
  - Los servicios tercerizados formarán parte de su programa normal de supervisión.
  - Se encuentra sujeta a principios, estándares o normas prevención del Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) internacionalmente aceptados, entre otros los difundidos por el Grupo de Acción Financiera Internacional (FATF-GAFI) y el Comité de Supervisión Bancaria de Basilea.
  - Además, respecto de la forma de supervisión, que adhiere a los “Principios básicos para una supervisión bancaria eficaz”, divulgados por el Comité de Supervisión Bancaria de Basilea. Y también aplica supervisión consolidada asumiendo la vigilancia de la liquidez y solvencia, así como la evaluación y el control de los riesgos y situaciones patrimoniales considerados en forma consolidada.

10.2. 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 tercerizados 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 tercerización.
- Procedimientos para la selección y contratación de terceras partes.
- La identificación y documentación de los servicios y actividades tercerizados.
- 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 tercerizados.
- La continuidad de los servicios de acuerdo con los resultados de los análisis de riesgos.
- La evaluación continua del nivel de exposición a los riesgos durante todo el ciclo de vida de la tercerización.
- 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.

Durante todo el ciclo de vida de la tercerización, cualquier cambio vinculado con la naturaleza de la actividad, la ubicación geográfica donde se realizan las actividades o las tareas de control, así como también la incorporación y/o modificaciones de las subcontrataciones (“n-ésimas partes”), deberá interpretarse como un nuevo proceso de tercerización y deberá cumplir con todos los requisitos contemplados en el punto 10.1.

Los cambios relevantes en la tercerización en el exterior de servicios críticos intra-grupo deberán contar con una nueva certificación escrita del supervisor del país de origen prevista en el punto 10.1.

10.3. Formalización de la relación.

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

- La naturaleza, el alcance de los procesos, servicios y/o actividades a tercerizar y las responsabilidades de las partes.
- La duración de la contratación o tercerización 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 a la entidad y a la SEFYC, en todos sus niveles de contratación, a requerir información precisa, completa y oportuna relacionada con los servicios tercerizados cuando lo estimen conveniente y el acceso irrestricto para auditar y obtener información relevante en las instalaciones, áreas de control y documentación sobre todos los prestadores de servicios.
- 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 tercerizados.
- La designación formal de un responsable en representación de la tercera parte para el tratamiento de aspectos vinculados con la tercerización, 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 servicios de mensajería financiera serán evaluados teniendo en cuenta sus condiciones particulares de contratación como por ejemplo SWIFT.

10.3.2. Subcontrataciones de las terceras partes.

Los documentos que instrumenten la contratación o tercerización deberán establecer formalmente la responsabilidad del prestador primario respecto de:

- Todos los procesos, servicios y/o actividades prestados 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 SEFYC.

10.4. Control y monitoreo.

Las entidades deberán definir un proceso de control de acuerdo con la evaluación de riesgos que les permita realizar un seguimiento y evaluación de los procesos, servicios y actividades de tecnología y seguridad de la información tercerizados.

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 tercerizados.

10.4.1. Informes de terceros independientes

Los informes de las evaluaciones realizadas por terceros independientes sobre los procesos, servicios y actividades tercerizados 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.

10.5. Informes de auditoría interna y externa.

Se deberán realizar auditorías internas sobre los procesos, servicios y actividades tercerizados que incluyan revisiones del cumplimiento de los requisitos legales y regulatorios.

La periodicidad de los informes de auditoría deberá definirse de acuerdo con el nivel de riesgo y la criticidad de los servicios o actividades tercerizados evaluando su impacto en el sistema de control interno de la entidad.

Conjuntamente con los informes de auditoría interna, 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 tercerizados.

Deberán encontrarse disponibles para la SEFYC, en todo momento:

- Los informes de los auditores internos y externos corporativos sobre los servicios tercerizados intra-grupo.

- Los informes de auditoría sobre los distintos prestadores de servicios tercerizados extra-grupo.

En todos los casos, la auditoría interna de la entidad local deberá analizar los informes de las auditorias recibidos y evaluar la razonabilidad, consistencia e integridad respecto del cumplimiento de las normativas locales vigentes para determinar, en todo momento, el mantenimiento de las condiciones iniciales tenidas en cuenta al contratar dichos servicios.

10.6. Consideraciones adicionales.

10.6.1. Los gastos en que incurra la SEFYC para realizar las inspecciones de la actividad tercerizada en el exterior del país (pasajes, alojamiento, viáticos, traslados, otros) deberán ser cubiertos en su totalidad por la entidad.

10.6.2. La tercera parte del exterior en la que se tercerice deberá estar constituida en países que estén sujetos a principios, estándares o normas sobre prevención del Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) internacionalmente aceptados, entre otros los difundidos por el Grupo de Acción Financiera Internacional (FATF-GAFI).

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 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.

Servicios críticos: aquellos que resulten esenciales para el funcionamiento continuo del sistema financiero y de la entidad, y para el cumplimiento de las obligaciones legales y regulatorias.

***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 (n-ésima parte) parte de lo que se le ha encomendado.

Tercera parte: quien brinda procesos, servicios y/o actividades tercerizados por la entidad.

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.

A partir del 04/08/26, los Proveedores de servicios de pago (PSP) incluidos en el Registro de PSP del Banco Central de la República Argentina deberán implementar esta normativa.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

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

TEXTO ORDENADO			NORMA DE ORIGEN				OBSERVACIONES
Sección	Punto	Párrafo	Com.	Cap.	Punto	Párrafo	
1.	1.1.		“A” 7724		2.		Según Com. “A” 7783 y 8398.
	1.2.		“A” 7724		2.		
2.	2.1.		“A” 7724		2.		
	2.2.		“A” 7724		2.		
	2.3.		“A” 7724		2.		
3.			“A” 7724		2.		
4.	4.1.		“A” 7724		2.		
	4.2.		“A” 7724		2.		
	4.3.		“A” 7724		2.		
	4.4		“A” 7724		2.		
	4.5.		“A” 7724		2.		
	4.6.		“A” 7724		2.		
	4.7.		“A” 7724		2.		
5.	5.1.		“A” 7724		2.		
	5.2.		“A” 7724		2.		
	5.3.		“A” 7724		2.		
	5.4.		“A” 7724		2.		
	5.5.		“A” 7724		2.		
	5.6.		“A” 7724		2.		
	5.7.		“A” 7724		2.		
	5.8.		“A” 7724		2.		
6.	6.1.		“A” 7724		2.		
	6.2.		“A” 7724		2.		
	6.3.		“A” 7724		2.		
	6.4.		“A” 7724		2.		
	6.5.		“A” 7724		2.		
	6.6.		“A” 7724		2.		
	6.7.		“A” 7724		2.		
	6.8.		“A” 7724		2.		
7.	7.1.		“A” 7724		2.		
	7.2.		“A” 7724		2.		
	7.3.		“A” 7724		2.		
	7.4.		“A” 7724		2.		
	7.5.		“A” 7724		2.		
	7.6.		“A” 7724		2.		
	7.7.		“A” 7724		2.		
8.	8.1.		“A” 7724		2.		
	8.2.		“A” 7724		2.		
	8.3.		“A” 7724		2.		
9.	9.1.		“A” 7724		2.		
	9.2.		“A” 7724		2.		
10.	10.1.		“A” 8398		3.		
	10.2.		“A” 7724		2.		Según Com. “A” 8398.
	10.3.		“A” 7724		2.		Según Com. “A” 8398.
	10.4.		“A” 7724		2.		Según Com. “A” 8398.
	10.5.		“A” 7724		2.		Según Com. “A” 8398.
	10.6.		“A” 8398		3.		

REQUISITOS MÍNIMOS PARA LA GESTIÓN Y CONTROL DE LOS RIESGOS DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN							
TEXTO ORDENADO			NORMA DE ORIGEN				OBSERVACIONES
Sección	Punto	Párrafo	Com.	Cap.	Punto	Párrafo	
11.			“A” 7724		2.		Según Com. “A” 8398.
12.			“A” 8398		1.		

Comunicaciones que componen el historial de la norma

Últimas modificaciones:

02/06/23: "A" 7783

13/02/26: "A" 8401

Últimas versiones de la norma - Actualización hasta:

28/11/23

13/02/26

Texto base:

Comunicación "A" 7724: Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información

Comunicaciones que dieron origen y/o actualizaron esta norma:

"A" 3198: Requisitos operativos mínimos del área de sistemas de información (SI) - tecnología informática. Texto ordenado.

"A" 4609: Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información.

"A" 4690: Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con Tecnología Informática y Sistemas de Información. Modificaciones.

"A" 5374: 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". Modificación.

"A" 6017: "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras". Modificaciones.

"A" 6209: Categorización de localidades para entidades financieras. Texto ordenado.

"A" 6290: Autorización y composición del capital de entidades financieras. Autoridades de entidades financieras. Adecuaciones.

"A" 6375: "Expansión de entidades financieras" y "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras". Actualización.

"A" 6684: Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras". Adecuaciones

"A" 7319: Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras. Adecuaciones.

“A” 7325: Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras.

“A” 7370: Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras. Adecuaciones.

“A” 7777: Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información. Texto ordenado.

“A” 7783: Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información”. Adecuaciones. “Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información asociados a los servicios financieros digitales”. Reglamentación.

“A” 8398: Requisitos Mínimos para la Gestión y Control de los Riesgos de Tecnología y Seguridad de la Información. Expansión de Entidades Financieras. Adecuaciones.

“A” 8401: Requisitos Mínimos para la Gestión y Control de los Riesgos de Tecnología y Seguridad de la Información. Expansión de Entidades Financieras. Actualización.