



BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" 8315	01/09/2025
-----------------------	------------

A LAS ENTIDADES FINANCIERAS:

Ref.: Circular
LISOL 1-1116,
RUNOR 1-1918:

Lineamientos para la Gestión de Riesgos en las Entidades Financieras. Distribución de Resultados. Actualización de textos ordenados.

Nos dirigimos a Uds. para hacerles llegar en anexo las hojas que, en reemplazo de las oportunamente provistas, corresponde incorporar en el texto ordenado sobre Lineamientos para la Gestión de Riesgos en las Entidades Financieras, atento a lo dispuesto por la resolución difundida por la Comunicación A 8249.

Asimismo, se actualiza el punto 3.4. del texto ordenado sobre Distribución de Resultados como consecuencia de lo previsto por la Comunicación A 8204.

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

Saludamos a Uds. atentamente.

BANCO CENTRAL DE LA REPÚBLICA ARGENTINA

Ana M. Dentone
Subgerenta de Regulaciones
Técnico - Prudenciales

Darío C. Stefanelli
Gerente Principal de Emisión
y Aplicaciones Normativas

ANEXO



-Índice-

Sección 6. Gestión del riesgo operacional.

- 6.1. Conceptos.
- 6.2. Responsabilidades.
- 6.3. Proceso de gestión del riesgo operacional.
- 6.4. Gestión de riesgos de tecnología y seguridad de la información.
- 6.5. Transparencia.

Sección 7. Gestión del riesgo de titulización.

- 7.1. Consideraciones generales.
- 7.2. Proceso de gestión del riesgo de titulización.
- 7.3. Operaciones relacionadas con las titulizaciones.
- 7.4. Riesgos residuales.
- 7.5. Transparencia.

Sección 8. Gestión del riesgo de concentración.

- 8.1. Conceptos.
- 8.2. Situaciones que pueden originar concentraciones de riesgo.
- 8.3. Marco para la gestión del riesgo de concentración.
- 8.4. Proceso de gestión del riesgo de concentración.
- 8.5. Pruebas de estrés. Responsabilidades.
- 8.6. Transparencia.

Sección 9. Gestión del riesgo reputacional.

- 9.1. Conceptos.
- 9.2. Proceso de gestión del riesgo reputacional.
- 9.3. Transparencia.

Sección 10. Gestión del riesgo estratégico.

- 10.1. Concepto.
- 10.2. Proceso de gestión del riesgo estratégico.
- 10.3. Responsabilidades.
- 10.4. Transparencia.

Sección 11. Realización de pruebas de estrés.

- 11.1. Conceptos.
- 11.2. Lineamientos.



-Índice-

Sección 12. Resiliencia operacional.

- 12.1. Conceptos.
- 12.2. Responsabilidades.
- 12.3. Gestión del riesgo operacional.
- 12.4. Planificación y testeo de la continuidad del negocio.
- 12.5. Mapeo de interconexiones e interdependencias.
- 12.6. Gestión de la dependencia de terceras partes (tercerización).
- 12.7. Gestión de incidentes.
- 12.8. Tecnología y seguridad de la información.

Tabla de correlaciones



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

Las entidades financieras deben implementar un marco para gestionar el riesgo operacional como una disciplina integral y separada de los restantes riesgos, el cual debe ser proporcional a las dimensiones de la entidad y a la complejidad de sus operatorias y adecuado a su perfil de riesgo.

6.1. Conceptos.

6.1.1. Riesgo operacional.

Se entiende por riesgo operacional –concepto que incluye el riesgo legal y excluye el riesgo estratégico y de reputación–, al riesgo de pérdidas resultantes de la falta de adecuación o fallas en los procesos internos, de la actuación del personal o de los sistemas o bien aquellas que sean producto de eventos externos.

El riesgo legal, que puede verificarse en forma endógena o exógena a la entidad financiera comprende, entre otros aspectos, la exposición a sanciones, penalidades u otras consecuencias económicas y de otra índole por incumplimiento de normas y obligaciones contractuales.

Se entiende por riesgo estratégico al procedente de una estrategia de negocios inadecuada o de un cambio adverso en las previsiones, parámetros, objetivos y otras funciones que respaldan esa estrategia.

Cada entidad podrá adoptar a su criterio una definición de riesgo operacional más amplia, adecuándola a su realidad y necesidades, siempre que, como mínimo, se incluyan los conceptos contemplados precedentemente.

6.1.2. Gestión del riesgo operacional.

Se entiende por gestión del riesgo operacional a la identificación, evaluación, seguimiento, control y mitigación de este riesgo.

Las entidades financieras deben evaluar su vulnerabilidad ante los eventos, para así comprender mejor su perfil de riesgo operacional y, en su caso, adoptar las medidas correctivas de las políticas que sean pertinentes.

El marco para la gestión del riesgo operacional comprende las políticas, prácticas, procedimientos y estructuras con que cuenta la entidad financiera para su adecuada gestión, debiendo además permitirle evaluar la suficiencia del capital. El marco debe cubrir el apetito y la tolerancia al riesgo operacional de la entidad –lo cual debe estar establecido en las políticas de gestión de este riesgo–, incluyendo el grado y el modo en que este riesgo se transfiere fuera de la entidad.

6.1.3. Eventos de pérdida.

Se indica a continuación la lista taxativa de las categorías –a los fines de las presentes disposiciones– para la clasificación de los eventos de pérdida derivados del riesgo operacional, incluyendo algunos ejemplos de los conceptos que integrarían cada una de ellas:



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

- 6.1.3.1. Fraude interno: información falsa sobre posiciones –propias o de clientes–, robos por parte de empleados, utilización de información confidencial de la entidad financiera en beneficio del empleado, etc.
- 6.1.3.2. Fraude externo: robo, falsificación, daños por intromisión en los sistemas informáticos, etc.
- 6.1.3.3. Relaciones laborales y seguridad en el puesto de trabajo: reclamos de indemnizaciones por parte de los empleados, infracciones a las normas laborales de seguridad e higiene, de discriminación, responsabilidades generales, etc.
- 6.1.3.4. Prácticas con los clientes, productos y negocios: abuso de información confidencial sobre el cliente, negociación fraudulenta en las cuentas de la entidad financiera, lavado de dinero, venta de productos no autorizados, etc.
- 6.1.3.5. Daños a activos físicos derivados de: actos de terrorismo y vandalismo, terremotos, incendios, inundaciones, etc.
- 6.1.3.6. Alteraciones en la actividad y fallas tecnológicas: fallas del *hardware* o del *software*, problemas en las telecomunicaciones, interrupción en la prestación de servicios públicos, etc.
- 6.1.3.7. Ejecución, gestión y cumplimiento del plazo de los procesos: errores en la introducción de datos, fallas en la administración de garantías, documentación jurídica incompleta, concesión de acceso no autorizado a las cuentas de los clientes, litigios con proveedores, etc.

Un mismo evento de pérdida no podrá registrarse en más de una de las categorías mencionadas precedentemente.

6.1.4. Líneas de defensa.

Las entidades financieras generalmente se apoyan en 3 líneas de defensa, cuyo grado de implementación debe ser proporcional a la naturaleza, la dimensión de la entidad y la complejidad de sus operatorias y adecuado a su perfil de riesgo.

- i) Primera línea: gestión en las unidades de negocio –tales como finanzas, recursos humanos, tecnología– cuyas responsabilidades, entre otras, son identificar y evaluar los riesgos operacionales significativos inherentes a sus respectivas unidades de negocios, establecer controles apropiados para mitigarlos y evaluar el diseño y efectividad de esos controles mediante el uso de herramientas de gestión.
- ii) Segunda línea: gestión independiente del riesgo operacional, que desarrolla una visión independiente de las unidades de negocios con respecto a los riesgos operacionales significativos identificados, el diseño y la efectividad de los controles clave y la tolerancia al riesgo. Además, entre otras responsabilidades, revisa la relevancia y consistencia de la implementación por parte de las unidades de negocios de las herramientas de gestión del riesgo operacional, las actividades de medición y los sistemas de informes.

Versión: 3a.	COMUNICACIÓN “A” 8315	Vigencia: 01/09/2025	Página 2
--------------	-----------------------	-------------------------	----------



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

- iii) Tercera línea: revisión independiente que asegura que el marco de gestión del riesgo operacional sea adecuado. Generalmente, recae en la auditoría interna y/o externa. Entre otras responsabilidades, debe revisar el diseño y la implementación de los sistemas de gestión del riesgo operacional y los procesos de gobierno asociados en la primera y segunda línea de defensa, así como los procesos de validación para garantizar su independencia e implementación consistente con las políticas de la entidad.

Si en las unidades de negocio existen funciones de la primera y segunda línea de defensa, las entidades deberán documentar y delimitar las responsabilidades de cada función, remarcando la independencia de la segunda línea.

6.2. Responsabilidades.

Corresponderá a cada entidad implementar una administración eficiente del riesgo operacional, considerando los lineamientos que se exponen a continuación y teniendo en cuenta las dimensiones de la entidad y la complejidad de sus operatorias.

El Directorio, la Alta Gerencia y la unidad encargada o persona responsable de la gestión del riesgo operacional, deberán evidenciar alto grado de compromiso tendiente a mantener una sólida cultura de la gestión del riesgo operacional en la cual las actividades relacionadas con ese riesgo formen parte de los procesos diarios de la entidad financiera.

6.2.1. Directorio.

El Directorio será responsable de que la entidad cuente con una estrategia adecuada para la gestión del riesgo operacional, del riesgo operacional asumido por la entidad y de la forma en que se gestiona. Para ello deberá:

- 6.2.1.1. Aprobar el marco que se utilizará para la gestión del riesgo operacional cuya periodicidad mínima de revisión será anual o cada vez que se produzcan, a juicio de la entidad, hechos o situaciones de relevancia vinculadas con este riesgo, los cuales deberán ser puestos en conocimiento de la Superintendencia de Entidades Financieras y Cambiarias;
- 6.2.1.2. Tener un claro conocimiento de los procedimientos desarrollados a efectos de gestionar el riesgo operacional y su grado de cumplimiento. Para ello, deberá recibir, como mínimo semestralmente, información suficiente que permita analizar el perfil de riesgo operacional general de la entidad financiera y verificar las implicancias estratégicas y sustanciales para su actividad;
- 6.2.1.3. Asegurar que el marco para la gestión del riesgo operacional esté sujeto a un proceso de auditoría interna –área que no será responsable de su gestión– que contemple una adecuada cobertura y profundidad de las revisiones y la adopción oportuna de medidas correctivas por parte de las áreas auditadas;
- 6.2.1.4. Aprobar políticas de difusión del marco de gestión del riesgo operacional y de capacitación, dirigidas a todas las áreas y funcionarios de la entidad financiera;

Versión: 4a.	COMUNICACIÓN “A” 8315	Vigencia: 01/09/2025	Página 3
--------------	-----------------------	-------------------------	----------



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

- 6.2.1.5. Establecer políticas para la gestión de los riesgos operacionales derivados de las actividades tercerizadas, de las actividades delegadas con ajuste a lo previsto en la Sección 9. del TO sobre Expansión de Entidades Financieras y de los servicios prestados por los proveedores;
- 6.2.1.6. Aprobar una política para la difusión a terceros de la información que corresponda sobre el marco de gestión del riesgo operacional. El contenido de dicha información y sus características serán proporcionales al volumen, complejidad y perfil de riesgo de las operaciones de la entidad financiera;
- 6.2.1.7. Garantizar que la entidad cuente con personal técnicamente calificado, así como también con los recursos necesarios para la gestión del riesgo operacional;
- 6.2.1.8. Verificar que los encargados de esa gestión –unidad de riesgo operacional o persona responsable, conforme al punto 6.2.4.– no desarrollen otras tareas en áreas que puedan generar conflictos de intereses con su función;
- 6.2.1.9. Aprobar y revisar periódicamente la definición del apetito y la tolerancia al riesgo operacional en línea con la naturaleza, tipos y niveles de riesgo operacional que la entidad financiera está dispuesta a asumir.

La definición del apetito y la tolerancia al riesgo operacional de la entidad debe estar vinculada con sus planes estratégicos y financieros de corto y largo plazo. Teniendo en cuenta tanto los intereses de los clientes y accionistas de la entidad como los requisitos regulatorios, una definición efectiva del apetito y la tolerancia al riesgo debe:

- i) ser fácil de comunicar y de entender para todas las partes interesadas;
- ii) incluir antecedentes y supuestos que contemplen los planes de negocios de la entidad;
- iii) incluir los motivos para asumir o evitar ciertos tipos de riesgos, y los límites o indicadores (que pueden ser cuantitativos o no) para permitir el seguimiento de estos riesgos;
- iv) asegurar que la estrategia y los límites de riesgo de las unidades de negocio, los demás entes que conforman el grupo económico de la entidad y las terceras partes contratadas (tercerizadas), según corresponda, se alinean con el apetito al riesgo establecido por la entidad financiera; y
- v) ser prospectiva y, de ser posible, estar sujeta a escenarios y pruebas de estrés que aseguren que la entidad entiende cuáles son los eventos que podrían llevarla a exceder su apetito y tolerancia al riesgo.

En la revisión de la adecuación de los límites y de la definición general del apetito y la tolerancia al riesgo, el Directorio deberá considerar: los cambios actuales y esperados en el ámbito externo –incluido el marco regulatorio en todas las jurisdicciones donde la entidad financiera presta servicios–; aumentos significativos actuales o futuros en los volúmenes de negocios o actividades; la



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

calidad del entorno de control; la eficacia de las estrategias de gestión o mitigación de los riesgos; experiencias de pérdida; y la frecuencia, el volumen o la naturaleza de los desvíos a los límites establecidos.

El Directorio deberá monitorear el cumplimiento de la definición del apetito y la tolerancia al riesgo y asegurar la oportuna detección y corrección de los desvíos.

6.2.1.10. Supervisar regularmente la eficacia de la gestión de riesgos de tecnología y seguridad de la información a los fines de asegurar la confidencialidad, integridad y disponibilidad de los datos y los sistemas.

6.2.2. Alta Gerencia.

6.2.2.1. Será la responsable de la implementación, reporte y control de los procesos y procedimientos para la puesta en práctica y funcionamiento del marco de gestión aprobado por el Directorio de la entidad. Ese marco será aplicado en forma consistente en toda la entidad financiera, debiendo todos los niveles de la organización comprender sus responsabilidades con respecto a la administración de este riesgo.

6.2.2.2. Será la encargada de que existan procesos y procedimientos aplicables a cada unidad de negocio, destinados a la gestión del riesgo operacional de los productos, actividades, procesos y sistemas de la entidad financiera.

6.2.2.3. Deberá establecer líneas claras de autoridad, responsabilidad y comunicación con las distintas gerencias para fomentar y mantener la asunción de responsabilidades.

6.2.2.4. Asegurará la existencia de recursos suficientes para la realización de una gestión eficaz del riesgo operacional.

6.2.2.5. Deberá evaluar si el proceso de vigilancia gerencial se adapta a los riesgos inherentes a las políticas de cada unidad de negocio.

6.2.2.6. Recibirá informes de la unidad de riesgo operacional o persona responsable y, en su caso, del nivel funcional con capacidad decisoria en materia de gestión de riesgos del cual dependa esa unidad o persona, relacionados con los resultados de la ejecución de los procesos y procedimientos, la detección de las posibles deficiencias que se produzcan en las políticas, procesos y procedimientos de gestión del riesgo operacional y las pertinentes propuestas para su corrección. La entidad financiera establecerá la periodicidad de los citados informes de acuerdo con su dimensión, la naturaleza y complejidad de sus productos y procesos y con la magnitud de sus operaciones.

6.2.2.7. Informará al Directorio, como mínimo semestralmente, sobre los principales aspectos relacionados con la gestión del riesgo operacional.



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

6.2.2.8. Evaluará regularmente el diseño, implementación y eficacia de la gestión de riesgos de tecnología y seguridad de la información.

6.2.2.9. Asegurará que el proceso de gestión del cambio en la entidad sea integral, cuente con los recursos adecuados y esté apropiadamente articulado entre las líneas de defensa pertinentes.

6.2.3. Gerencias.

Las gerencias serán responsables de aplicar, en las distintas unidades de negocios –según su ámbito de competencia– los procesos y procedimientos concretos conforme al marco definido para la gestión del riesgo operacional, debiéndose asegurar que tanto los procedimientos como los controles sean adecuados y eficaces en el ámbito que se apliquen.

Asimismo, informarán a la unidad de riesgo operacional o persona responsable acerca de los resultados de la ejecución de los procesos y procedimientos, con la periodicidad que la entidad financiera establezca de acuerdo con su dimensión, la naturaleza y complejidad de sus productos y procesos y con la magnitud de sus operaciones.

6.2.4. Unidad de riesgo operacional o persona responsable.

La estructura de la unidad encargada de la gestión del riesgo operacional contemplará las siguientes características:

6.2.4.1. Se adecuará a la dimensión de la entidad, la naturaleza y complejidad de sus productos y procesos y a la magnitud de sus operaciones;

6.2.4.2. Deberá depender funcionalmente de la Gerencia General –o autoridad equivalente– o de un nivel funcional con capacidad decisoria en materia de gestión de riesgos que reporte a esa Gerencia;

6.2.4.3. No podrá estar a cargo de la auditoría interna, área que –no obstante ello– podrá aportar sus conocimientos para el desarrollo del marco de gestión de riesgo operacional y para la constante mejora de su administración;

6.2.4.4. Podrá involucrar a personal de otras áreas siempre que las responsabilidades asignadas no impliquen conflictos de intereses en función de las respectivas incumbencias;

6.2.4.5. Existirá independencia entre la unidad o persona responsable de la gestión del riesgo operacional y las unidades de negocio involucradas, así como una clara delimitación de funciones, responsabilidades y perfil de puestos en todos sus niveles;

6.2.4.6. Deberá articular los principales procesos que la entidad financiera necesite para gestionar el riesgo operacional, adoptando los mecanismos que permitan una comunicación, interacción y coordinación efectiva con los responsables de los otros riesgos –que tenga la entidad conforme a sus definiciones y los requerimientos del Banco Central de la República Argentina– y de los responsables de contratar servicios externos;

Versión: 3a.	COMUNICACIÓN “A” 8315	Vigencia: 01/09/2025	Página 6
--------------	-----------------------	-------------------------	----------



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

6.2.4.7. Recibirá de las Gerencias informes con los resultados de la ejecución de los procesos y procedimientos, con la periodicidad que la entidad financiera establezca de acuerdo con su dimensión, la naturaleza y complejidad de sus productos y procesos y con la magnitud de sus operaciones;

6.2.4.8. Informará a la Gerencia General o, en su caso, al nivel funcional con capacidad decisoria en materia de gestión de riesgos del que dependa, la detección de las posibles deficiencias que se produzcan en la aplicación de las políticas, procesos y procedimientos de gestión del riesgo operacional y las pertinentes propuestas para su corrección, con la periodicidad que la entidad financiera establezca de acuerdo con su dimensión, la naturaleza y complejidad de sus productos y procesos y con la magnitud de sus operaciones.

6.3. Proceso de gestión del riesgo operacional.

Una gestión efectiva de este riesgo contribuirá a prevenir futuras pérdidas derivadas de eventos operativos. Consecuentemente, las entidades financieras deben gestionar el riesgo operacional inherente a sus productos, actividades, procesos y sistemas relevantes; además, en forma previa a un lanzamiento o presentación de nuevos productos, inicio de actividades, puesta en marcha de procesos o sistemas, también deben comprobar que se evalúa adecuadamente su riesgo operacional inherente.

El proceso de gestión del riesgo operacional comprenderá las etapas que se describen a continuación.

6.3.1. Identificación y evaluación.

6.3.1.1. Consideraciones generales.

Para la identificación del riesgo operacional, se tendrán en cuenta factores internos –tales como, la estructura de la entidad financiera y la naturaleza de sus actividades– y externos –tales como, cambios en el sector y avances tecnológicos–, que pudieran afectar el desarrollo de los procesos e influir negativamente en las proyecciones realizadas conforme a las estrategias de negocios definidas por la entidad financiera.

Las entidades financieras utilizarán datos internos, debiendo establecer un proceso para registrar y consignar en forma sistemática la frecuencia, severidad, categorías y otros aspectos relevantes de los eventos de pérdida por riesgo operacional.

La registración de esos eventos contribuirá a reducir los incidentes, las pérdidas y a mejorar la calidad del servicio y de los productos.

El proceso de recolección de datos deberá ser acompañado de una política de incentivos que permita fomentar su registración, promoviendo de este modo una cultura organizacional para el reporte de tales datos y de controles que contribuyan a la verificación de su consistencia e integridad.



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

6.3.1.2. Herramientas.

Entre las herramientas que las entidades deberán utilizar para identificar y evaluar sus riesgos operacionales pueden destacarse:

- i) Autoevaluación de sus riesgos operacionales. Consiste en evaluar el riesgo inherente –antes de realizar los controles y medidas de mitigación–, la eficacia del entorno de control y el riesgo residual –después de realizar los controles y medidas de mitigación– y comprende tanto elementos cuantitativos como cualitativos.

Las evaluaciones deben utilizar el mapeo de los procesos de negocio para identificar los pasos claves en esos procesos, actividades y funciones de la organización, así como los riesgos asociados y las áreas donde existen debilidades en el control. Deberán contener información suficientemente detallada sobre el entorno empresarial, riesgos operacionales, causas subyacentes, controles y evaluación de la eficacia del control.

Las entidades deberán mantener un registro de riesgos operacionales a los fines de tener una visión significativa de la eficacia general de los controles y para facilitar la supervisión por parte de la Alta Gerencia, los comités de riesgos y el Directorio.

- ii) Base de datos de eventos de riesgo operacional. Recopilación de todos los eventos significativos ocurridos utilizados como base para las evaluaciones del riesgo operacional. Incluye datos de pérdidas internas, cuasipérdidas y, de ser posible, datos de eventos de pérdidas operacionales externas; la fecha del evento –fechas de ocurrencia, de descubrimiento y de contabilización–; el impacto financiero en el caso de eventos de pérdida, y cualquier otra información sobre la causa de los eventos.
- iii) Gestión de eventos. Incluye al análisis de eventos para identificar nuevos riesgos operacionales, comprender las causas subyacentes y las debilidades en el control, y formular una respuesta adecuada para prevenir la recurrencia de eventos similares. Esta información se utiliza para la autoevaluación y, en particular, para la evaluación de la eficacia del control.
- iv) Marco de monitoreo y pruebas de control. El análisis debe considerar la suficiencia del control, incluidas las estrategias adecuadas de prevención, detección y respuesta. El seguimiento y las pruebas de control deben ser apropiados para los diferentes riesgos operacionales y los controles clave en todas las áreas de negocio.
- v) Métricas. En el desarrollo de métricas se deben utilizar los datos de eventos de riesgo operacional y las evaluaciones de riesgo y de control para evaluar y monitorear su exposición a ese riesgo.

Las métricas brindan información de alerta temprana para monitorear el desempeño continuo del negocio y el entorno de control, y para informar el perfil de riesgo operacional.



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

- vi) Análisis de escenarios. Método para identificar, analizar y medir distintos escenarios, incluidos eventos de baja probabilidad y de alta gravedad, algunos de los cuales podrían ocasionar pérdidas severas por riesgo operacional.

El análisis de escenarios generalmente implica reuniones de expertos en la materia, incluidas la Alta Gerencia, las gerencias y personal senior de riesgo operacional y otras áreas funcionales como recursos humanos, cumplimiento y gestión de riesgos de tecnología y seguridad de la información, para desarrollar y analizar las causas y las consecuencias de los eventos potenciales.

En el análisis de escenarios se incluyen datos relevantes de pérdidas internas y externas, información de autoevaluaciones, el marco de pruebas de control y monitoreo de control, métricas prospectivas, análisis de la causa y el marco del proceso, cuando se utilice.

El proceso de análisis de escenarios podría usarse para desarrollar una serie de consecuencias de eventos potenciales, incluidas las evaluaciones de impacto para la gestión de riesgos, complementando otras herramientas basadas en datos históricos o evaluaciones de riesgos actuales. También podría integrarse con los planes de continuidad del negocio y recuperación, para su uso dentro de las pruebas de resiliencia operacional.

- vii) Evaluación y análisis comparativo. Son comparaciones de los resultados provenientes de diferentes herramientas de gestión y medición de riesgos implementadas dentro de la entidad.

Las entidades financieras deberán asegurarse de que los resultados de las herramientas para la evaluación del riesgo operacional estén:

- a) basados en datos precisos, cuya integridad esté garantizada por un gobierno y procedimientos de verificación y validación sólidos;
- b) considerados en la fijación de “precios” y la medición del rendimiento, así como en las evaluaciones de oportunidades de negocio; y
- c) sujetos a planes de acción monitoreados en el marco de gestión del riesgo operacional o planes de recuperación, cuando sea necesario.

Estas herramientas también pueden contribuir directamente al enfoque de resiliencia operacional de la entidad financiera, en particular, los procedimientos de gestión de eventos, autoevaluación y análisis de escenarios, ya que permiten identificar y monitorear amenazas y vulnerabilidades a sus operaciones críticas.

Las entidades deberán usar los resultados de estas herramientas para mejorar sus controles y procedimientos de resiliencia operacional.



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

6.3.1.3. Proceso de gestión del cambio.

Las entidades financieras deberán contar políticas y procedimientos de gestión del cambio que definan el proceso para identificar, gestionar, aprobar y monitorear el cambio sobre la base de criterios objetivos acordados. Los cambios pueden consistir en participar de nuevas actividades o desarrollar nuevos productos o servicios, entrar en mercados o jurisdicciones desconocidos, implementar nuevos procesos de negocio o sistemas tecnológicos o modificarlos y/o participar en negocios que están geográficamente distantes de la casa matriz. La gestión del cambio debe evaluar la evolución de los riesgos asociados a lo largo del tiempo.

La implementación de los cambios debe ser monitoreada por controles específicos. Las políticas y los procedimientos de gestión del cambio deben estar sujetos a revisiones y actualizaciones periódicas e independientes y asignar claramente las funciones y responsabilidades de acuerdo con el modelo de las 3 líneas de defensa, en particular:

- i) La primera línea de defensa debe realizar evaluaciones del control y riesgo operacional de nuevos productos, actividades, procesos y sistemas, incluida la identificación y evaluación del cambio requerido a través de las fases de toma de decisiones y la planificación para la implementación y la posterior revisión.
- ii) La segunda línea de defensa debe revisar las evaluaciones del control y del riesgo operacional de la primera línea de defensa, así como monitorear la implementación de controles apropiados o medidas correctivas. Esta línea de defensa debe cubrir todas las fases de este proceso y asegurar que todas las áreas de control relevantes –finanzas, cumplimiento, jurídica, comercial, de tecnología, gestión de riesgos, entre otras– estén involucradas, según corresponda.

Las entidades financieras deberán tener políticas y procedimientos para la revisión y aprobación de nuevos productos, actividades, procesos y sistemas. El proceso de revisión y aprobación debe considerar:

- a) Los riesgos inherentes, incluidos los riesgos legales, de tecnología y seguridad de la información y de modelo, en el lanzamiento de nuevos productos, servicios, actividades y operaciones en mercados desconocidos, y en la implementación de nuevos procesos, personas y sistemas –especialmente en el caso de la tercerización de servicios–;
- b) los cambios en el perfil, apetito y tolerancia al riesgo operacional, incluyendo cambios en el riesgo de productos o actividades existentes;
- c) los controles necesarios, los procesos de gestión de riesgos y las estrategias de mitigación de riesgos;
- d) el riesgo residual;
- e) cambios en los umbrales o límites de riesgo; y



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

- f) los procedimientos y métricas para evaluar, monitorear y gestionar el riesgo de nuevos productos, servicios, actividades, mercados, jurisdicciones, procesos y sistemas.

El proceso de revisión y aprobación debe asegurar que se ha realizado la inversión adecuada en recursos humanos e infraestructura tecnológica antes de que se introduzcan los cambios.

Los cambios deben monitorearse, durante y después de su implementación, para identificar cualquier diferencia significativa con respecto al perfil de riesgo operacional esperado y gestionar cualquier riesgo inesperado.

Las entidades financieras deberán mantener un registro central de sus productos y servicios –incluidos los tercerizados– para facilitar el seguimiento de los cambios.

6.3.2. Seguimiento.

Las entidades financieras deben contar con un proceso de seguimiento eficaz a los efectos de facilitar la rápida detección y corrección de las posibles deficiencias que se produzcan en sus políticas, procesos y procedimientos de gestión del riesgo operacional. Este proceso debe insertarse en las actividades habituales de la entidad financiera.

Además del seguimiento de los eventos de pérdidas operativas, las entidades financieras deben verificar la evolución de los indicadores a los fines de reformularlos en función de la naturaleza de los eventos de pérdida producidos.

La unidad encargada o persona responsable de la gestión del riesgo operacional deberá remitir al Gerente General –o autoridad equivalente– o, en su caso, al nivel funcional con capacidad decisoria en materia de gestión de riesgos del cual dependa, con la periodicidad que la entidad financiera establezca de acuerdo con su dimensión, la naturaleza y complejidad de sus productos y procesos y con la magnitud de sus operaciones, informes vinculados a los resultados del seguimiento realizado y las pertinentes propuestas de corrección en los procesos y procedimientos.

Los informes mencionados precedentemente, una vez analizados por la Gerencia General y aprobadas las correcciones pertinentes, se distribuirán entre los niveles gerenciales correspondientes y las áreas de la entidad financiera que pudieran verse afectadas, a fin de que adopten esas medidas correctivas para asegurar una gestión eficaz del riesgo operacional.

6.3.3. Control y mitigación.

Las entidades deberán tener un entorno de control sólido que utilice políticas, procesos y sistemas, controles internos adecuados y estrategias apropiadas de mitigación y/o transferencia de riesgos operacionales.



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

6.3.3.1. Los controles internos deben estar diseñados para asegurar que la entidad financiera tendrá operaciones eficientes y efectivas, salvaguardar sus bienes, producir informes financieros confiables y cumplir con las leyes y regulaciones aplicables.

Un adecuado programa de control interno consta de 4 componentes que son parte integral del proceso de gestión de riesgos: a) evaluación de riesgos; b) actividades de control; c) información y comunicación; y d) actividades de seguimiento.

Los procesos y procedimientos de control deben incluir un sistema que asegure el cumplimiento de las políticas, regulaciones y leyes.

La evaluación del cumplimiento de las políticas contempla, entre otros aspectos:

- i) Las revisiones de alto nivel sobre el progreso respecto de los objetivos establecidos.
- ii) La verificación del cumplimiento de los controles de gestión.
- iii) La revisión del tratamiento y resolución de los incumplimientos.
- iv) La evaluación de las aprobaciones y autorizaciones requeridas para asegurar responsabilidad de acuerdo con un nivel apropiado de gestión.
- v) El seguimiento de los informes de las excepciones aprobadas con respecto a umbrales o límites, gestión de anulaciones y otras desviaciones a las políticas, regulaciones y leyes.

Los procesos y procedimientos de control deben abordar la forma en que la entidad financiera asegura su resiliencia operacional tanto en situaciones normales como en casos de disrupción, reflejando la debida diligencia de las respectivas funciones, de conformidad con el enfoque de resiliencia operacional de la entidad.

Un entorno de control efectivo también requiere la separación adecuada de las responsabilidades con controles duales. Los conflictos de intereses deben identificarse, minimizarse y sujetarse a un cuidadoso control y revisión independientes.

Asimismo, las entidades financieras deberán asegurarse de que existan otros controles internos, según corresponda, para abordar el riesgo operacional, tales como:

- a) autoridades y/o procesos de aprobación claramente establecidos;
- b) monitoreo del cumplimiento de los umbrales o límites de riesgo establecidos;
- c) protección para el acceso y el uso de los activos y registros de la entidad;
- d) idoneidad del personal y capacitación para mantener la experiencia técnica;

Versión: 1a.	COMUNICACIÓN "A" 8315	Vigencia: 01/09/2025	Página 12
--------------	-----------------------	-------------------------	-----------



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

- e) procesos continuos para identificar las unidades de negocio o productos en los cuales los rendimientos parecen no estar en línea con expectativas razonables;
- f) verificación periódica y conciliación de transacciones y cuentas; y
- g) política de vacaciones que disponga que los funcionarios y empleados se ausentarán –sin comunicación con ningún agente de la entidad (ni conexión remota o de otro tipo)– por un período no inferior a 2 semanas consecutivas.

El uso efectivo y la implementación sólida de la tecnología pueden contribuir al entorno de control. Las entidades deben tener un enfoque integrado para identificar, evaluar, seguir, controlar y mitigar los riesgos tecnológicos en línea con los lineamientos para la gestión del riesgo operacional. En relación con los aspectos vinculados a la tecnología informática, resultarán de aplicación las regulaciones específicas vigentes en materia de tecnología y seguridad de la información.

En los casos en que los controles internos no aborden adecuadamente el riesgo, la entidad podrá buscar transferir el riesgo, utilizando herramientas o programas de cobertura de riesgo como, por ejemplo, pólizas de seguro, las cuales deberán ser usadas como complemento de las medidas de control interno, pero no deberán ser consideradas como sustitutos de la gestión del riesgo operacional. El Directorio deberá determinar la exposición máxima a pérdidas que la entidad financiera esté dispuesta y tenga la capacidad financiera de asumir, y deberá realizar una revisión anual del programa de gestión de riesgos y seguros de la entidad.

6.3.3.2. Riesgo de tercerización.

Las políticas de gestión del riesgo de tercerización como parte de las políticas del marco de gestión del riesgo operacional, y las actividades para la gestión de los riesgos deben contemplar:

- i) procedimientos para determinar si las actividades pueden ser contratadas (tercerizadas) y de qué manera;
- ii) procesos de debida diligencia en la selección de potenciales proveedores de servicios;
- iii) estructuración sólida del acuerdo de tercerización, incluida la propiedad y la confidencialidad de los datos, así como los derechos de rescisión;
- iv) programas de gestión y seguimiento de los riesgos asociados a la tercerización, incluida la situación financiera del prestador del servicio;
- v) entorno de control efectivo en la entidad y en el proveedor de servicios, que debe incluir un registro de actividades contratadas (tercerizadas), así como métricas y reportes para facilitar la supervisión del proveedor de servicios;
- vi) desarrollo de planes de contingencia viables;

Versión: 1a.	COMUNICACIÓN “A” 8315	Vigencia: 01/09/2025	Página 13
--------------	-----------------------	-------------------------	-----------



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

vii) celebración de contratos integrales y/o acuerdos de nivel de servicio con una clara asignación de responsabilidades entre el tercero proveedor de servicios y la entidad financiera; y

viii) acceso de la entidad financiera a la supervisión de terceras partes contratadas (tercerizadas).

El Directorio y la Alta Gerencia serán responsables de comprender los riesgos operacionales asociados con la tercerización y de asegurar que se implementen políticas y prácticas efectivas de gestión de riesgos en las actividades de tercerización, teniendo en cuenta, entre otros aspectos, la concentración de riesgo y la complejidad de esas actividades.

6.3.4. Plan de continuidad del negocio.

Las entidades financieras deberán contar con planes de continuidad del negocio que aseguren su capacidad de operar de manera continua y limiten sus pérdidas en caso de interrupción severa del negocio. Los planes de continuidad del negocio deben estar en línea con lo establecido en la Sección 12. en materia de Resiliencia Operacional y el marco de gestión del riesgo operacional de la entidad.

Una sólida y efectiva política de continuidad del negocio requiere:

- i) su revisión periódica y aprobación del Directorio;
- ii) el involucramiento sólido de la Alta Gerencia y del personal con capacidad decisoria de las unidades de negocio en su implementación;
- iii) el compromiso de la primera y segunda línea de defensa en su diseño; y
- iv) la revisión periódica por parte de la tercera línea de defensa.

Las entidades deberán elaborar planes de continuidad del negocio prospectivos que incluyan análisis de escenarios asociados a evaluaciones de impacto relevantes y procedimientos de recuperación. Para su elaboración, se deberá tener en cuenta que:

- a) la política de continuidad del negocio debe estar basada en el análisis de escenarios de potenciales interrupciones que identifiquen y clasifiquen las operaciones críticas del negocio y las áreas internas y externas claves, debiendo cubrir todas sus unidades de negocio, así como sus proveedores críticos y terceras partes importantes –tales como bancos centrales, cámaras de compensación, procesadoras de operaciones con tarjetas de crédito, administradoras de redes de cajeros automáticos, banca por internet y banca móvil–;
- b) cada escenario debe estar sujeto a una evaluación de impacto cuantitativa y cualitativa con respecto a sus consecuencias financieras, operacionales, legales y reputacionales;



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

- c) los escenarios de disrupción deben estar sujetos a umbrales o límites para la activación de un procedimiento de continuidad del negocio, el cual debe incluir aspectos de reanudación, objetivos y tiempo de recuperación, así como guías de comunicación a las gerencias, los empleados, las autoridades reguladoras y los clientes; y
- d) los escenarios que contemplen tecnología y seguridad de la información deben considerar los lineamientos regulatorios específicos vigentes e integrarse con el resto de la gestión de continuidad del negocio.

Las entidades deberán revisar periódicamente sus planes y políticas de continuidad del negocio para asegurar que las estrategias de contingencia son consistentes con las operaciones, los riesgos y las amenazas actuales.

Los programas de capacitación y concientización deben personalizarse basándose en los roles específicos para garantizar que el personal pueda ejecutar planes de contingencia de manera efectiva.

Los procedimientos de continuidad del negocio deben probarse periódicamente para asegurar que se pueden cumplir los objetivos y los plazos de recuperación y reanudación. Siempre que sea posible, la entidad deberá participar en las pruebas de continuidad del negocio con los proveedores de servicios claves. Los resultados de las pruebas formales y las actividades de revisión deberán informarse a la Alta Gerencia y al Directorio.

6.4. Gestión de riesgos de tecnología y seguridad de la información.

Las entidades financieras deberán implementar un programa sólido de gestión de riesgos de tecnología y seguridad de la información en línea con el marco de gestión del riesgo operacional.

El uso adecuado y la implementación de una sólida gestión de riesgos de tecnología y seguridad de la información son primordiales para que las entidades realicen su negocio adecuadamente, contribuyen a la eficacia del entorno de control y son fundamentales para el logro de sus objetivos estratégicos. La evaluación de estos riesgos debe asegurar que la tecnología de la información respalde y facilite las operaciones.

La gestión de riesgos de tecnología y seguridad de la información debe reducir la exposición al riesgo operacional por pérdidas directas, reclamos legales, daño reputacional, de disrupción y uso indebido de la tecnología en línea con el nivel del apetito y la tolerancia al riesgo definido por la entidad. Esta gestión incluye:

- i) la identificación y evaluación de los riesgos de tecnología y seguridad de la información;
- ii) las medidas de mitigación de esos riesgos consistentes con el nivel de riesgo evaluado –tales como programas de respuesta y recuperación, procesos de gestión del cambio, procesos de gestión de incidentes, incluyendo la comunicación de información relevante y oportuna a los usuarios–; y



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

iii) el monitoreo de esas medidas de mitigación, incluyendo pruebas periódicas.

A los fines de asegurar la confidencialidad, integridad y disponibilidad de los datos y los sistemas, además de las responsabilidades del Directorio y de la Alta Gerencia previstas en el punto 6.2., se requiere la alineación regular de las estrategias del negocio, de la gestión de riesgos y de la tecnología y seguridad de la información para que sean consistentes con el apetito y la tolerancia al riesgo definidos por la entidad y con la regulación sobre protección de datos personales.

Las entidades deberán monitorear continuamente su gestión de tecnología y seguridad de la información y reportar regularmente a la Alta Gerencia sobre riesgos, controles y eventos.

La gestión de riesgos de tecnología y seguridad de la información debe:

- a) ser revisada regularmente para adecuarse a estándares y buenas prácticas del sistema financiero, así como frente a amenazas –tales como cibernéticas– y a tecnologías nuevas o en desarrollo;
- b) ser regularmente testeada como parte de un programa para identificar desvíos en relación con los objetivos de tolerancia al riesgo establecidos, y facilitar la mejora de la identificación de riesgos de tecnología y seguridad de la información, su protección, detección y gestión de eventos; y
- c) hacer uso de la inteligencia de amenazas para la mejora continua de la concientización sobre las vulnerabilidades de los sistemas, redes y aplicaciones y facilitar la toma de decisiones sobre la gestión de riesgos o ante los cambios.

Las entidades deberán estar preparadas para escenarios de estrés que contemplen eventos externos disruptivos, tales como la necesidad de facilitar la implementación de acceso remoto a gran escala, el despliegue rápido de activos físicos y/o la expansión del ancho de banda de conectividad para soportar las conexiones de usuarios y la protección de los datos de sus clientes.

En ese sentido, las entidades financieras deberán asegurar que:

- se desarrollen estrategias apropiadas para mitigar potenciales riesgos asociados con una disrupción o compromiso de los sistemas, redes o aplicaciones. Se deberá evaluar si los riesgos, junto con esas estrategias, son acordes con su apetito y tolerancia al riesgo;
- estén bien definidos los procesos para la gestión de los usuarios y que exista un desarrollo correcto de las aplicaciones; y
- se realicen actualizaciones periódicas de la tecnología y seguridad de la información, incluyendo los aspectos referidos a ciberseguridad, para lograr un nivel de seguridad adecuado.

6.5. Transparencia.

Las entidades financieras deberán dar a conocer al público –de manera regular– a través de sus páginas de Internet o reportes, la evaluación de su enfoque de gestión del riesgo operacional y su exposición a ese riesgo.

Versión: 1a.	COMUNICACIÓN “A” 8315	Vigencia: 01/09/2025	Página 16
--------------	-----------------------	-------------------------	-----------



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 6. Gestión del riesgo operacional.

A tales efectos, las entidades financieras deberán:

- i) divulgar información relevante sobre su exposición al riesgo operacional a las partes interesadas –incluidos los eventos de pérdida operacional significativa–.

La divulgación debe ser proporcional –en cantidad y tipo de información– al tamaño, perfil de riesgo y complejidad de sus operaciones y a la evolución de la práctica en el sistema financiero;

- ii) divulgar su marco de gestión del riesgo operacional de manera que permita a las partes interesadas determinar si la entidad identifica, evalúa, sigue, controla y mitiga el riesgo operacional de manera eficaz;
- iii) tener una política de divulgación formal que esté sujeta a una revisión regular e independiente y a la aprobación de la Alta Gerencia y el Directorio. Esta política debe contemplar el enfoque de la entidad para determinar qué divulgaciones sobre riesgo operacional realizará y los controles internos sobre el proceso de divulgación; e
- iv) implementar un proceso para evaluar la conveniencia de sus divulgaciones y su política de divulgación.



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 12. Resiliencia operacional.

La resiliencia operacional de una entidad financiera es su capacidad para continuar con sus operaciones críticas durante situaciones disruptivas de cualquier naturaleza.

Al considerar su resiliencia operacional, las entidades financieras deberán asumir que pueden producirse interrupciones, identificar cuáles son sus operaciones críticas, y tener en cuenta su apetito general al riesgo y su tolerancia a la interrupción.

12.1. Conceptos.

12.1.1. Tolerancia a la interrupción: nivel de interrupción que una entidad financiera está dispuesta a aceptar sin dejar de cumplir con sus operaciones críticas dada una serie de posibles escenarios severos de interrupción.

12.1.2. Operaciones críticas: incluyen actividades, procesos, servicios y sus estructuras de apoyo –personas, tecnología, información e instalaciones– cuya falla daría lugar a la interrupción de servicios que son esenciales para el funcionamiento continuo de la entidad y su rol en el sistema financiero (tales como pagos, custodia, préstamos, depósitos, etc.).

12.1.3. Funciones para la gestión del riesgo operacional: a los fines de estas disposiciones, se entiende por funciones a las 3 líneas de defensa descriptas en la Sección 6.

12.2. Responsabilidades.

Las entidades deberán utilizar su estructura de gobierno para establecer, supervisar e implementar un enfoque efectivo de resiliencia operacional que les permita responder y adaptarse a eventos disruptivos, así como recuperarse y aprender de ellos a fin de minimizar su impacto en la provisión de operaciones críticas.

12.2.1. Directorio.

El Directorio deberá:

12.2.1.1. Revisar y aprobar el enfoque de resiliencia operacional de la entidad financiera considerando su apetito al riesgo y la tolerancia a la interrupción de sus operaciones críticas. Al formular la tolerancia a la interrupción, debe tener en cuenta las capacidades operativas de la entidad para una amplia serie de probables escenarios severos que podrían afectar sus operaciones críticas.

12.2.1.2. Asegurar que las políticas consideren de manera efectiva los casos en los que las capacidades de la entidad financiera sean insuficientes para cumplir con su tolerancia a la interrupción.

12.2.1.3. Desempeñar un papel activo para asegurar una comprensión amplia del enfoque de resiliencia operacional de la entidad, a través de la comunicación clara de sus objetivos a todas las partes relevantes, incluido el personal, terceras partes y entidades pertenecientes al grupo económico.



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 12. Resiliencia operacional.

12.2.2. Alta Gerencia.

La Alta Gerencia deberá:

12.2.2.1. Implementar el enfoque de resiliencia operacional de la entidad y asegurar que los recursos –financieros y técnicos, entre otros– se asignen de manera adecuada para respaldar ese enfoque.

12.2.2.2. Proporcionar informes periódicos y oportunos sobre la resiliencia operacional de las unidades de negocios para apoyar la supervisión del Directorio, particularmente en los casos en que deficiencias significativas puedan afectar la ejecución de las operaciones críticas de la entidad financiera.

12.3. Gestión del riesgo operacional.

Las entidades financieras deberán apoyarse en sus funciones para la gestión del riesgo operacional a los fines de identificar de manera continua las amenazas externas e internas y fallas potenciales en las personas, infraestructura, procesos y sistemas, evaluar rápidamente las vulnerabilidades de las operaciones críticas y gestionar los riesgos resultantes de acuerdo con su enfoque de resiliencia operacional.

La función de gestión del riesgo operacional deberá trabajar junto con otras funciones relevantes para gestionar y abordar cualquier riesgo que amenace la ejecución de operaciones críticas. Para fortalecer la resiliencia operacional en toda la entidad, se deberá coordinar la planificación de la continuidad del negocio, la gestión de la dependencia de terceras partes (tercerización), la planificación de la recuperación y reanudación y otros marcos de gestión de riesgos relevantes.

Las entidades financieras deberán contar con controles y procedimientos para identificar y evaluar de manera oportuna las amenazas y vulnerabilidades y, en general, su riesgo operacional y, en la medida de lo posible, evitar que afecten la ejecución de operaciones críticas.

Las funciones respectivas deberán evaluar periódicamente la eficacia de los controles y procedimientos implementados. Estas evaluaciones también deberán realizarse en caso de cambios en cualquier componente interno de las operaciones críticas, así como después de producidos los incidentes para aprender de ellos y tener en cuenta las nuevas amenazas y vulnerabilidades que causaron los incidentes y los cambios.

Las entidades financieras deberán aprovechar sus capacidades para gestionar los cambios en el marco de la gestión integral de riesgo operacional como una forma de evaluar los efectos potenciales en las operaciones críticas y en sus interconexiones e interdependencias.

12.4. Planificación y testeo de la continuidad del negocio.

Las entidades financieras deberán contar con planes y ejercicios de continuidad del negocio que incluyan una serie de posibles escenarios severos, a fin de probar su capacidad para ejecutar sus operaciones críticas durante situaciones disruptivas.

Versión: 1a.	COMUNICACIÓN “A” 8315	Vigencia: 01/09/2025	Página 2
--------------	-----------------------	-------------------------	----------



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 12. Resiliencia operacional.

Un plan de continuidad de negocios efectivo debe:

- i) ser prospectivo al evaluar el impacto de potenciales interrupciones. Los ejercicios de continuidad del negocio deben realizarse y validarse para una serie de probables escenarios severos que incluyan eventos e incidentes disruptivos;
- ii) identificar las operaciones críticas y las dependencias internas y externas claves para evaluar los riesgos y el impacto potencial de distintos escenarios de interrupción en esas operaciones críticas;
- iii) incorporar un análisis del impacto de esas posibles interrupciones en el negocio y estrategias de recuperación, así como programas de prueba, simulacros, validaciones, programas de capacitación y concientización, y programas de comunicación y gestión de crisis;
- iv) desarrollar, implementar y realizar regularmente ejercicios de continuidad del negocio que comprendan las operaciones críticas y sus interconexiones e interdependencias, incluidas, entre otras, aquellas con terceras partes y entidades pertenecientes al grupo económico. Estos ejercicios deben ayudar a la concientización del personal sobre la resiliencia operacional, incluida su capacitación para que puedan adaptarse y responder de manera efectiva a los incidentes;
- v) proporcionar una guía detallada y clara respecto de:
 - a) la implementación del marco de recuperación ante desastres, estableciendo las funciones y las responsabilidades para gestionar las interrupciones operativas;
 - b) la sucesión de la autoridad en caso de que una interrupción afecte al personal clave; y
- vi) establecer claramente el proceso interno de toma de decisiones y definir los incidentes o eventos que pueden activar el plan de continuidad del negocio.

Un plan de continuidad de negocios para la ejecución de operaciones y servicios críticos provistos por terceras partes debe ser consistente con el enfoque de resiliencia operacional.

Los escenarios que contemplan tecnología y seguridad de la información deberán considerar las regulaciones específicas vigentes e integrarse con el resto de la gestión de continuidad del negocio.

12.5. Mapeo de interconexiones e interdependencias.

Las entidades financieras, una vez que han identificado sus operaciones críticas, deberán mapear las interconexiones e interdependencias internas y externas necesarias para la provisión de estas operaciones, de manera consistente con su enfoque de resiliencia operacional.



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 12. Resiliencia operacional.

Las respectivas funciones deberán mapear –identificar, analizar y documentar– las personas, la tecnología, los procesos, la información, las instalaciones y las interconexiones e interdependencias entre ellos, necesarios para realizar las operaciones críticas de la entidad, incluidas aquellas que dependen de, pero no se limitan a, terceras partes o acuerdos con el grupo económico al que pertenecen (por ejemplo, agencias complementarias de servicios financieros, contrapartes con la que se celebren acuerdos de cobranzas extrabancarias, de adquisición de cartera de créditos, etc.).

Las entidades financieras podrán utilizar sus planes de recuperación y reanudación, según corresponda, para las definiciones de operaciones críticas y deberán considerar si sus enfoques de resiliencia operacional están adecuadamente armonizados con los mapeos de sus operaciones críticas y de los servicios críticos de terceras partes contenidos en sus planes de recuperación y reanudación.

El enfoque y el nivel de granularidad del mapeo deben ser suficientes para que las entidades identifiquen las vulnerabilidades y respalden las pruebas de su capacidad para realizar las operaciones críticas durante situaciones disruptivas, considerando su apetito al riesgo y tolerancia a la interrupción.

12.6. Gestión de la dependencia de terceras partes (tercerización).

Las entidades financieras deberán:

- 12.6.1. Gestionar sus dependencias respecto de sus relaciones con terceras partes, incluyendo, entre otras, aquellas con entidades pertenecientes a su grupo económico, para la provisión de operaciones críticas.
- 12.6.2. Realizar la evaluación de riesgos y la debida diligencia antes de celebrar acuerdos con terceras partes (tercerización) –incluidos, entre otros, proveedores críticos o entidades pertenecientes al grupo económico–, de conformidad con el marco de gestión del riesgo operacional, la política de gestión de riesgos de tercerización y el enfoque de resiliencia operacional.
- 12.6.3. Verificar, previamente a la celebración del acuerdo, si esa tercera parte tiene al menos un nivel equivalente de resiliencia operacional para salvaguardar las operaciones críticas de la entidad tanto en circunstancias normales como en casos de interrupción.
- 12.6.4. Desarrollar planes de contingencia y continuidad del negocio que incluyan las estrategias para mantener la capacidad de recuperación operativa de la entidad financiera en caso de una falla o interrupción en un tercero que afecte la prestación de las operaciones críticas. Los escenarios utilizados deben evaluar la sustituibilidad de las terceras partes que brindan servicios a las operaciones críticas de la entidad y otras alternativas viables para facilitar el restablecimiento del servicio.



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 12. Resiliencia operacional.

12.7. Gestión de incidentes.

Las entidades financieras deberán desarrollar e implementar planes de respuesta y de recuperación para gestionar incidentes que podrían alterar la ejecución de las operaciones críticas, en línea con su apetito al riesgo y su tolerancia a la disrupción. Estos planes deberán ser mejorados continuamente mediante la incorporación del aprendizaje que surge de incidentes anteriores.

Las entidades financieras deberán mantener un inventario de las respuestas y de la recuperación ante incidentes, y de recursos internos y de terceras partes, para respaldar las capacidades de respuesta y recuperación.

La gestión de incidentes debe considerar el ciclo de vida de un incidente, que normalmente incluye, entre otros:

- i) la clasificación de la gravedad del incidente basada en criterios predefinidos –tales como el tiempo esperado para volver a funcionar normalmente–, lo que permite la priorización adecuada y la asignación de recursos para responder ante un incidente;
- ii) los procedimientos de respuesta y recuperación ante incidentes, incluida su vinculación con la continuidad del negocio, recuperación ante desastres, otros planes y procedimientos de contingencia y gestión asociados;
- iii) la implementación de planes de comunicación para reportar los incidentes a las partes interesadas internas y externas –por ejemplo, autoridades reguladoras–, incluidas las métricas de desempeño durante el incidente y el análisis posterior del evento.

Los procedimientos de respuesta y recuperación ante incidentes deberán revisarse, testearse y actualizarse periódicamente. Las entidades deberán identificar y abordar las causas de los incidentes para prevenir o minimizar la recurrencia en serie. Esto incluye, entre otros, los incidentes atribuibles a las terceras partes y entidades pertenecientes al grupo económico.

Los aspectos relativos a la gestión de ciberincidentes deberán considerar las regulaciones específicas vigentes e integrarse con el resto de la gestión de incidentes.

12.8. Tecnología y seguridad de la información.

Las entidades financieras deberán garantizar que la tecnología y la seguridad de la información sean resilientes, sujetas a procesos de protección, detección, respuesta y recuperación testeados regularmente, que incorporen un adecuado conocimiento de la situación y transmitan información relevante y oportuna para la gestión de riesgos y la toma de decisiones, a fin de facilitar la provisión de las operaciones críticas.



B.C.R.A.	LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS
	Sección 12. Resiliencia operacional.

Las entidades deberán:

- 12.8.1. Tener una política de tecnología documentada, incluida la gestión de la seguridad de la información, que establezca los requisitos vinculados con gobierno y supervisión, responsabilidad y propiedad del riesgo, medidas de seguridad –tales como, controles de acceso, protección de activos de información críticos, gestión de identidad–, evaluación periódica y seguimiento de los controles de ciberseguridad, respuesta a incidentes, planes de continuidad del negocio y recuperación ante desastres.
- 12.8.2. Identificar sus activos de información críticos y la infraestructura de la que dependen. Además, las entidades financieras deberán:
- i) priorizar los esfuerzos de seguridad de la información en función de su evaluación de riesgos de tecnología y seguridad de la información, y en la importancia de los activos de información críticos para las operaciones críticas, al tiempo que deben cumplir con todos los requisitos legales y regulatorios relacionados con la protección de datos;
 - ii) desarrollar planes e implementar controles para mantener la integridad de la información crítica en caso de un evento de seguridad, como almacenamiento seguro y respaldo fuera de línea en medios inmutables de datos que respaldan operaciones críticas; y
 - iii) evaluar periódicamente el perfil de amenaza de sus activos de información críticos, testear las vulnerabilidades y garantizar su resistencia a los riesgos de tecnología y seguridad de la información.



LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS							
TEXTO ORDENADO			NORMA DE ORIGEN				OBSERVACIONES
Sección	Punto	Párrafo	Com.	Cap.	Punto	Párrafo	
5.	5.5.		“A” 6397		1.		
	5.6.		“A” 6397		1.		
	5.7.		“A” 5203				Según Com. “A” 6397.
6.		1°	“A” 4793				Según Com. “A” 5203 y 5398.
	6.1.1.		“A” 4793				Según Com. “A” 5203 y 5398.
	6.1.2.		“A” 4793				Según Com. “A” 5203, 5398 y 8249.
	6.1.3.		“A” 4793				
	6.1.4.		“A” 8249				
	6.2.	1°	“A” 4793				
	6.2.	2°	“A” 4793				Según Com. “A” 4854, 5203 y 5398.
	6.2.1.		“A” 4793				Según Com. “A” 5203, 5398, 6603 y 8249.
	6.2.2.		“A” 4793				Según Com. “A” 4854, 5203 y 8249.
	6.2.3.		“A” 4793				Según Com. “A” 5203 y 5398.
	6.2.4.		“A” 4793				Según Com. “A” 4854 y 5203.
	6.3.	1°	“A” 4793				Según Com. “A” 5203 y 5398.
	6.3.1.		“A” 4793				Según Com. “A” 5398 y 8249.
	6.3.2.		“A” 4793				Según Com. “A” 4854, 5203 y 5398.
	6.3.3.		“A” 4793				Según Com. “A” 4854, 5203, 5398 y 8249.
	6.3.4.		“A” 8249				
	6.4.		“A” 8249				
	6.5.		“A” 8249				
7.	7.1.		“A” 5398				Según Com. “A” 6327.
	7.2.		“A” 5398				
	7.3.		“A” 5398				
	7.3.3.		“A” 5398				Según Com. “A” 6433.
	7.4.		“A” 5398				
	7.5.		“A” 5398				
8.	8.1.		“A” 5398				
	8.2.		“A” 5398				
	8.3.		“A” 5398				
	8.4.		“A” 5398				
	8.5.		“A” 5398				
	8.6.		“A” 5398				
9.	9.1.		“A” 5398				
	9.2.		“A” 5398				
	9.3.		“A” 5398				
10.	10.1.		“A” 5398				
	10.2.		“A” 5398				
	10.3.		“A” 5398				
	10.4.		“A” 5398				
11.	11.1.		“A” 5203				
	11.2.		“A” 5203				Según Com. “A” 5398.



LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS EN LAS ENTIDADES FINANCIERAS							
TEXTO ORDENADO			NORMA DE ORIGEN				OBSERVACIONES
Sección	Punto	Párrafo	Com.	Cap.	Punto	Párrafo	
12.	12.1.		"A" 8249				
	12.2.		"A" 8249				
	12.3.		"A" 8249				
	12.4.		"A" 8249				
	12.5.		"A" 8249				
	12.6.		"A" 8249				
	12.7.		"A" 8249				
	12.8.		"A" 8249				



B.C.R.A.	DISTRIBUCIÓN DE RESULTADOS
	Sección 3. Verificación de liquidez y solvencia.

El importe a distribuir, que no podrá superar el determinado en la Sección 2., no deberá comprometer la liquidez y solvencia de la entidad. Este requisito se considerará cumplido cuando se verifique la inexistencia de defectos de integración en la posición de capital mínimo –tanto individual como consolidada– del cierre del ejercicio al que correspondan los resultados no asignados considerados o en la última posición cerrada, de ambas la que presente menor exceso de integración respecto de la exigencia, recalculándolas computando además –a ese único fin– los siguientes efectos en función de los correspondientes datos a cada una de esas fechas:

- 3.1. Los resultantes de la deducción del activo de los conceptos mencionados en los puntos 2.1. a 2.5., de corresponder.
- 3.2. La no consideración de las franquicias otorgadas por la SEFYC que afecten las exigencias, integraciones o la posición de capital mínimo.
- 3.3. La deducción de los resultados no asignados de los importes correspondientes a los siguientes conceptos:
 - 3.3.1. el importe a distribuir y, en su caso, el que se destine a constituir la reserva a los fines de retribuir instrumentos representativos de deuda, susceptibles de integrar la responsabilidad patrimonial computable;
 - 3.3.2. saldos a favor por aplicación del impuesto a la ganancia mínima presunta –netos de las provisiones por riesgo de desvalorización– que no hayan sido deducidos del patrimonio neto básico, conforme a lo establecido en el TO sobre Capitales Mínimos de las Entidades Financieras; y
 - 3.3.3. ajustes efectuados según los puntos 2.1. a 2.5.
- 3.4. La no consideración del límite previsto en el punto 7.3. del TO sobre Capitales Mínimos de las Entidades Financieras.

Sin perjuicio de lo establecido precedentemente, sólo se admitirá la distribución de resultados en la medida que no se verifique alguna de las siguientes condiciones:

- se encuentren alcanzadas por las disposiciones de los artículos 34 “Regularización y saneamiento” y 35 bis “Reestructuración de la entidad en resguardo del crédito y los depósitos bancarios” de la Ley de Entidades Financieras;
- registren asistencia financiera por iliquidez del BCRA, en el marco del artículo 17 de su Carta Orgánica;
- presenten atrasos o incumplimientos en el régimen informativo establecido por esta Institución;
- registren deficiencias de integración de capital mínimo –de manera individual o consolidada– (sin computar a tales fines los efectos de las franquicias individuales otorgadas por la SEFYC);



B.C.R.A.	ORIGEN DE LAS DISPOSICIONES CONTENIDAS EN EL TEXTO ORDENADO SOBRE DISTRIBUCIÓN DE RESULTADOS
----------	---

TEXTO ORDENADO			NORMA DE ORIGEN						OBSERVACIONES
Secc.	Punto	Párr.	Com.	Anexo	Cap.	Secc.	Punto	Párr.	
1.			"A" 4589				1.		Según Com. "A" 5827 y 6464.
2.		1° y 2°	"A" 4589				2.		Según Com. "A" 4591 (punto 6.), 5273, 5827, 6327 y 6464.
	2.1.		"A" 6327				12.		
	2.2.		"A" 6396				4.		
	2.3.		"A" 6327				12.		
	2.4.		"A" 4589				2.3.		
	2.5.		"A" 4589				2.4.		
3.		último	"A" 6327				26.		
		1°	"A" 4589				3.		Según Com. "A" 4591 (punto 8.), 5072, 5273, 5827, 5985, 6464 y "B" 9104.
	3.1.		"A" 4589				3.1.		Según Com. "A" 4591 (punto 8.) y 6428.
	3.2.		"A" 4589				3.3.	iv)	Según Com. "A" 4591 (punto 8.) y "B" 9104.
	3.3.		"A" 4589				3.3.		Según Com. "A" 4591 (punto 8.), 6428 y 6464.
	3.4.		"A" 5737				4.		Según Com. "A" 8204.
4.		último	"A" 4589				1.1. a 1.4.		Según Com "A" 4591, 5072 y 6464.
			"A" 5827						
5.			"A" 4591				1.		Según Com. "A" 5282 y 5827.
	5.1.		"A" 4591				1.		Incorpora el criterio interpretativo de la Com. "C" 46841. Según Com. "A" 5393.
	5.2.		"A" 4591				1.		Según Com. "A" 4686, 4702, 5072, 5180, 5282, 5369, 5580, 5827, 6013, 6464 y "B" 9104.
6.			"A" 6768						
7.	7.1.		"A" 5938						
	7.2.		"A" 6946				3.		Según Com. "A" 7007, 7108, 7143, 7181, 7427, 7659 y 7928.
	7.3.		"A" 6939						Según Com. "A" 7007, 7035, 7181, 7312, 7421, 7659, 7719, 7984 y 8214.
	7.4.		"A" 8235						