BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" **8249**	**02/06/2025**

A LAS ENTIDADES FINANCIERAS:

Ref.: Circular
LISOL 1-1102,
RUNOR 1-1900:

Lineamientos para la Gestión de Riesgos en las Entidades Financieras. Gestión del Riesgo Operacional. Resiliencia Operacional.

Nos dirigimos a Uds. para comunicarles que esta Institución adoptó la resolución que, en su parte pertinente, establece:

"1- Incorporar en el punto 6.1. del texto ordenado sobre Lineamientos para la Gestión de Riesgos en las Entidades Financieras lo siguiente:

"Las entidades financieras generalmente se apoyan en 3 (tres) 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.

- 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.

- 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.

- 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 la 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."

2- Disponer que, dentro de las responsabilidades del Directorio y de la Alta Gerencia previstas en los puntos 6.2.1. y 6.2.2., respectivamente, del texto ordenado sobre Lineamientos para la Gestión de Riesgos en las Entidades Financieras, se incorpore lo siguiente:

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

"- 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 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.

- 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."

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

- 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."

3- Sustituir las herramientas para identificar y evaluar los riesgos operacionales que se enumeran en el punto 6.3.1. del texto ordenado sobre Lineamientos para la Gestión de Riesgos en las Entidades Financieras, por las siguientes:

"- 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 ries-

go residual –después de realizar los controles y medidas de mitigación– y comprende tanto elementos cuantitativos como cualitativos.

Las evaluaciones deberán 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.

- 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, cuasi pérdidas 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.

- 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.

- 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.

- 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.

- 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.

- 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."

4- Incorporar en el punto 6.3.1. del texto ordenado sobre Lineamientos para la Gestión de Riesgos en las Entidades Financieras lo siguiente:

"Las entidades financieras deberán contar con 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 tres "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

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.”

5- Sustituir el punto 6.3.3. del texto ordenado sobre Lineamientos para la Gestión de Riesgos en las Entidades Financieras, por lo siguiente:

“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.

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 cuatro 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;

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 (dos) 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 dis-

puesta 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;

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- Incorporar en el punto 6.3. del texto ordenado sobre Lineamientos para la Gestión de Riesgos en las Entidades Financieras lo siguiente:

“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 disrupción severa del negocio. Los planes de continuidad del negocio deben estar en línea con lo previsto en el punto 9. de esta comunicación 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 disrupciones 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;

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.”

7- Disponer que en la Sección 6. del texto ordenado sobre Lineamientos para la Gestión de Riesgos en las Entidades Financieras se incorpore lo siguiente:

“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

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."

8- Incorporar en la Sección 6. del texto ordenado sobre Lineamientos para la Gestión de Riesgos en las Entidades Financieras lo siguiente:

"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.

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."

9- Incorporar en el texto ordenado sobre Lineamientos para la Gestión de Riesgos en las Entidades Financieras las disposiciones sobre resiliencia operacional contenidas en el Anexo, el cual forma parte de esta comunicación.

10- Disponer que las disposiciones contenidas en los puntos 1. a 9. de esta comunicación tengan vigencia a partir del 01/09/25."

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Asimismo, les informamos que posteriormente les haremos llegar las hojas que, en reemplazo de las oportunamente provistas, corresponderá incorporar en las normas de la referencia.

Saludamos a Uds. atentamente.

BANCO CENTRAL DE LA REPÚBLICA ARGENTINA

Darío C. Stefanelli
Gerente Principal de Emisión y
Aplicaciones Normativas

Marina Ongaro
Subgerenta General
de Regulación Financiera

ANEXO

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

B.C.R.A.	Lineamientos para la Gestión de Riesgos en las Entidades Financieras	Anexo a la Com. "A" 8249

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 disrupciones, identificar cuáles son sus operaciones críticas, y tener en cuenta su apetito general al riesgo y su tolerancia a la disrupción.

12.1. Conceptos.

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

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 disrupción 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 recuperase 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 disrupción de sus operaciones críticas. Al formular la tolerancia a la disrupción, 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 disrupción.

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.

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.

Un plan de continuidad de negocios efectivo debe:

i) ser prospectivo al evaluar el impacto de potenciales disrupciones. 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 disrupción en esas operaciones críticas;

iii) incorporar un análisis del impacto de esas posibles disrupciones 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 disrupciones operativas;

   b) la sucesión de la autoridad en caso de que una disrupción 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.

Las respectivas funciones deben 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 financie-

ros, 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 disrupción.

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 disrupción.

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 disrupción 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.

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 deben 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 deben 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.

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 res-

paldan 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.