LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO

TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS

CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO

(Capítulo sustituido por la Resolución No. SB-2018-771 de 30 de julio de 2018; reformado por Resolución No. SB-2018-814 de 13 de agosto de 2018; reformado por Resolución No. SB-2019-497 de 29 de abril de 2019; sustituido por la Resolución No. SB-2021-2126 de 02 de diciembre de 2021; reformado con Resolución No. SB-2021-2263 de 28 de diciembre de 2021 con la que sustituyó el nombre "Junta de Política y Regulación Monetaria y Financiera" por "Junta de Política y Regulación Financiera"; sustituido por la Resolución No. SB-2023-01901 de 12 de septiembre de 2023).

SECCIÓN I.- ÁMBITO, DEFINICIONES Y ALCANCE

ARTÍCULO 1.- Las disposiciones de la presente norma son aplicables a las entidades de los sectores financieros público y privado, a las cuales, en el texto de esta norma, se las denominará entidades controladas.

El marco de la administración del riesgo operativo es de responsabilidad del órgano de gobierno y de los comités relacionados de las entidades controladas.

Entiéndase como sector financiero público a los bancos y corporaciones y como sector financiero privado a los bancos múltiples, bancos especializados, entidades de servicios financieros y entidades de servicios auxiliares del sistema financiero, conforme el Código Orgánico Monetario y Financiero.

Para efecto de administrar adecuadamente el riesgo operativo, además de las disposiciones contenidas en la presente norma, las entidades controladas observarán las disposiciones de la "Política para la gestión integral y administración de riesgos de las entidades de los sectores financieros público y privado", emitida por la entonces Junta de Política y Regulación Monetaria y Financiera y la "Norma de control para la gestión integral y administración de riesgos de las entidades de los sectores financieros público y privado" emitida por la Superintendencia de Bancos.

Conforme a las atribuciones dispuestas en el artículo 63 del Código Orgánico Monetario y Financiero, la Superintendencia de Bancos podrá solicitar en cualquier momento, a cualquier entidad sometida a su control, la información que considere pertinente, sin límite alguno, en el ámbito de su competencia.

ARTÍCULO 2.- Para efectos de la aplicación de las disposiciones de la presente norma, se considerarán las siguientes definiciones:

1. Actividad.- Es el conjunto de tareas que ejecutan las entidades controladas.

2. Administración de la continuidad del negocio.- Es un proceso permanente que garantiza la continuidad de las operaciones de las entidades controladas, a través del mantenimiento efectivo de un sistema de gestión de continuidad del negocio.

3. Administración de la información.- Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes.

4. Alfanumérico.- Es el conjunto de caracteres conformado por letras y números.

5. Apetito al riesgo. - Es el nivel de exposición al riesgo operativo, definido por la entidad controlada, que está dispuesta a asumir o aceptar, en el desarrollo de sus operaciones con la finalidad de alcanzar sus objetivos estratégicos.

6. Aplicación informática.- Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones.

7. Banca electrónica.- Son los servicios suministrados por las entidades controladas a los clientes y/o usuarios, a través de protocolos de internet, indistintamente del dispositivo tecnológico del cual se acceda.

8. Banca móvil.- Son los servicios suministrados por las entidades controladas a los clientes y/o usuarios, a través de aplicaciones informáticas propias de los dispositivos móviles mediante los protocolos de estos equipos.

9. Cajeros automáticos (ATM).- Son máquinas conectadas informáticamente a una entidad controlada que permite efectuar al cliente ciertas transacciones.

10. Canales electrónicos.- Se refiere a todas las vías o formas a través de las cuales los clientes y/o usuarios pueden efectuar transacciones con las entidades controladas, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas, conforme a los tipos de canales (tabla 107) definidos en el manual de tablas de la normativa vigente de la Superintendencia de Bancos.

11. Capacidad al riesgo operativo .- Es el nivel máximo de riesgo operativo que la entidad financiera puede soportar sin que interfiera en la continuidad de las operaciones.

12. Causa raíz.- Es la causa principal que genera un incidente o problema; su identificación permite aplicar soluciones adecuadas, prevenir y resolver sistemáticamente la ocurrencia de incidente o problema, con el objetivo de evitar futuras ocurrencias.

13. Centro de procesamiento de datos.- Es la infraestructura que permite alojar los recursos relacionados con la tecnología que admite el procesamiento, almacenamiento y transmisión de la información.

14. Ciberseguridad.- Conjunto de medidas de protección de la infraestructura tecnológica y de la información, a través del tratamiento de las amenazas que ponen en riesgo la información procesada por los diferentes componentes tecnológicos interconectados.

15. Cifrar.- Es el proceso mediante el cual la información o archivos son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos al verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino.

16. Computación en la nube.- Es la provisión de servicios informáticos accesibles a través de la internet, estos pueden ser de infraestructura, plataforma y/o software.

17. Confidencialidad.- Es un principio y una práctica que se refiere a la protección y resguardo de la información sensible o privada para evitar su acceso o divulgación no autorizada.

18. Cumplimiento.- Se refiere a la observancia y aplicación de las leyes, reglamentos y demás normativa, así como los acuerdos contractuales en los procesos, actividades y operaciones a los que las entidades están sujetas.

19. Corresponsales no bancarios (CNB).- Son canales mediante los cuales las entidades de los sectores financieros público y privado, bajo su entera responsabilidad, pueden prestar sus servicios a través de terceros que estén conectados a la entidad financiera mediante sistemas

de transmisión de datos, previamente autorizados por el organismo de control, identificados y que cumplan con todas las condiciones de control interno, seguridades físicas y de tecnología de información, entre otras.

20. Datos.- Es cualquier forma de registro sea este electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido.

21. Datos personales.- Datos que identifican o hacen identificable a una persona natural, directa o indirectamente.

22. Disponibilidad.- Es el atributo de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios que satisfagan sus necesidades.

23. Evento de riesgo operativo.- Es el hecho que deriva en pérdidas para las entidades controladas, originado por fallas o insuficiencias en los factores de riesgo operativo.

24. Estándar ANSI TIA-942.- Guía que proporciona una serie de recomendaciones y directrices para la instalación de las infraestructuras de centros de procesamiento de datos en los aspectos de: telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico.

25. Factor de riesgo operativo.- Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son: procesos, personas, tecnología de la información y eventos externos.

26. Indicadores Claves de Riesgo.- Es una métrica que permite monitorear la exposición a un determinado riesgo, y ayudan a tomar acciones oportunas en el caso de desviaciones.

27. Información.- Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de un servicio.

28. Incidente.- Es una interrupción no planificada de un servicio o la reducción de su calidad, que afecta el normal funcionamiento de sus servicios.

29. Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones.

30. Insumo.- Es el conjunto de materiales, datos o información que sirven como entrada a un proceso.

31. Integridad.- Es el atributo de mantener la totalidad y exactitud de la información y de los métodos de procesamiento.

32. Línea de negocio.- Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo, definido en la planificación estratégica de la entidad.

33. Medios electrónicos.- Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares.

34. Mensajería Móvil.- Comunicación basada en mensajes a través de dispositivos móviles que permitan el registro, autenticidad y seguimiento a la trazabilidad.

35. Perfil de Riesgo Operativo.- Es el nivel del riesgo de la entidad que refleja la naturaleza y magnitud de los riesgos operativos a los que está expuesto.

36. Pista de auditoría.- Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos, bases de datos, sistemas operativos y demás elementos tecnológicos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría.

37. Plan de continuidad del negocio.- Es el conjunto de procedimientos que orientan a las entidades a mantener su operatividad en el caso de que ocurran interrupciones que afecten sus servicios.

38. POS y PIN Pad.- Son dispositivos de hardware y/o software fijos o móviles ubicados en puntos de venta que permiten realizar transacciones con tarjetas.

39. Primera línea de defensa.- Corresponde a la gestión operativa y de negocio que gestionan los riesgos operativos, responsables del control interno efectivo para identificar, evaluar, controlar, mitigar y notificar los riesgos asociados con sus actividades; de que existan controles adecuados; y, de que se sigan las políticas y procedimientos establecidos.

40. Problema.- Consecuencia de uno o varios incidentes críticos o un incidente que se repite muchas veces y por ello se debe encontrar su causa raíz.

41. Procedimiento.- Es la forma específica para llevar a cabo una actividad o un proceso.

42. Proceso.- Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente interno o externo utilizando recursos de la entidad.

43. Proceso crítico.- Es el conjunto de actividades indispensables para la continuidad del negocio y las operaciones de la entidad controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto negativo.

44. Propietario de la información.- Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de la información; debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidades.

45. Protección de datos personales. - Es un conjunto de prácticas de seguridad para evitar el uso indebido e ilegal de datos personales, para salvaguardarlos contra filtraciones, pérdida o compromiso de los datos.

46. Proveedor Sistémico. - Compañía que presta servicios a las entidades del sistema financiero que ante la posibilidad de que un evento o una serie de eventos pueda ocasionar una severidad con consecuencias sistemáticas.

47. Punto de recuperación objetivo (RPO).- Es la cantidad máxima aceptable de pérdida de los datos medidos en el tiempo.

48. Resiliencia Operativa. - Capacidad de una entidad para seguir entregando los servicios críticos durante eventos disruptivos; esta capacidad le permite a la entidad identificar y protegerse de amenazas y potenciales fallas, respondiendo y adaptándose a ellas; así como, recuperarse y aprender de los eventos disruptivos con la finalidad de minimizar su impacto hacia el futuro en la entrega de los servicios críticos.

49. Segunda línea de defensa. - Corresponde a las áreas especializadas, quienes establecen las políticas y estándares de riesgo operativo, monitorean y hacen contraposición de los controles diseñados y evaluados en la primera línea de defensa. También ayudan a definir y mantener el marco de gestión de riesgos de la organización y proporcionan un monitoreo independiente de la evolución de los riesgos.

50. Seguridad de la información. -Son los mecanismos adoptados por la entidad que le permiten preservar la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella, incluye los aspectos relacionados con ciberseguridad.

51. Sistema de audio respuesta (IVR).- Es un sistema automatizado de respuesta interactiva, orientado a entregar o recibir información a través del teléfono.

52. Tarea.- Es el conjunto de pasos que conducen a un resultado final visible y mesurable.

53. Tecnología de la información.- Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes y comunicaciones, entre otros.

54. Tarjeta con chip.- Es la tarjeta que posee circuitos integrados (chip) que permiten la ejecución de cierta lógica programada, contiene memoria y microprocesadores.

55. Tarjeta contactless.- Es la tarjeta que dispone de una tecnología NFC (Near Field Communication) que permite, a través de una comunicación inalámbrica de corto alcance y alta frecuencia, transaccionar al usuario con tan solo acercar la tarjeta a un terminal o lector.

56. Tercera línea de defensa.- Corresponde a la función de auditoría interna quien proporciona una evaluación independiente y objetiva de la eficacia global del marco de gobierno, riesgo y control de una organización. A través de su trabajo de auditoría, verifica si las dos primeras líneas de defensa son efectivas en la identificación, evaluación, control y monitoreo de los riesgos operativos.

57. Tiempo de recuperación objetivo (RTO).- Es el período de tiempo transcurrido después de un incidente, para reanudar una actividad o recuperar los recursos antes de que la entidad controlada genere pérdidas significativas.

58. TIER III.- Certificación o clasificación de los centros de datos que permite el mantenimiento concurrente, con una disponibilidad de 99.982% al año, y un tiempo de parada de 1.6 horas, e incluye redundancia en sus componentes de infraestructura, así como fuentes alternativas de electricidad y refrigeración en caso de emergencia.

59. Transacciones.- Son movimientos que realizan los clientes y/o usuarios a través de los canales que brindan las entidades; y pueden ser monetarias y no monetarias.

a) Transacciones monetarias.- Son las que implican movimiento de dinero y son realizadas por los clientes a través de canales presenciales o canales electrónicos, tales como: transferencias, depósitos, retiros, operaciones de crédito, pagos, recargas de telefonía móvil, entre otras.

b) Transacciones no monetarias.- Son las que no implican movimiento de dinero y son realizadas por los clientes a través de canales presenciales o canales electrónicos, tales como: consultas, cambios de clave, personalización de condiciones

60. Tolerancia al riesgo. Es el grado de desviación del riesgo operativo respecto del nivel de apetito de riesgo definido por el Directorio que la entidad puede soportar.

ARTÍCULO 3.- Para efectos de la presente norma, el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas por eventos derivados de fallas o insuficiencias en los factores de: procesos, personas, tecnología de la información y por eventos externos. El riesgo operativo incluye el riesgo legal, pero excluye los riesgos: sistémico, estratégico y de reputación.

El riesgo legal es la probabilidad de que las entidades controladas sufran pérdidas debido a que los activos y contingentes se encuentren expuestos a situaciones de mayor vulnerabilidad; que sus pasivos puedan verse incrementados más allá de los niveles esperados, o que el desarrollo

de sus operaciones enfrente la eventualidad de ser afectado negativamente, debido a error, negligencia, impericia, imprudencia o dolo, que deriven de la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales o normativas, así como de instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias; o, en sentencias o resoluciones jurisdiccionales o administrativas adversas; o, de la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos de las partes contratantes no han sido claramente estipulados.

SECCIÓN II.- ADMINISTRACION DEL RIESGO OPERATIVO

ARTÍCULO 4.- En el marco de la administración integral de riesgos, y alineado al apetito y tolerancia del riesgo definidos por la organización; la entidad controlada debe definir políticas, procesos, procedimientos y metodologías para la administración del riesgo operativo como un riesgo específico; y, definirán y adoptarán un modelo basado en el esquema de tres líneas de defensa considerando su objeto social, tamaño, naturaleza, complejidad de sus operaciones y demás características propias.

Las líneas de defensa relacionadas con el riesgo operativo de las entidades controladas deben cumplir y sin limitarse con las siguientes funciones:

1. Primera línea

a) Identificar y evaluar la materialidad de los riesgos operativos inherentes a su gestión de negocio y operativa mediante el uso de herramientas de gestión de riesgos operativos;
b) Establecer controles apropiados para mitigar los riesgos operativos inherentes y evaluar el diseño y la efectividad de estos controles;
c) Reportar los perfiles de riesgo operativo de la gestión de negocio y operativa;
d) Informar sobre los riesgos operativos residuales no mitigados por los controles, incluidos los eventos de pérdida, deficiencias de control, deficiencias de procesos y sus incumplimientos.

2. Segunda línea

a) Desarrollar una visión independiente con respecto a las unidades de negocio, identificar riesgos operativos, proponer controles clave y monitorear permanentemente el apetito y la tolerancia al riesgo operativo;
b) Evaluar periódicamente en la gestión de negocio y operativa la implementación de las metodologías o herramientas de gestión del riesgo operativo, manteniendo evidencias de la evaluación realizada;
c) Desarrollar y mantener políticas, estándares y directrices de gestión y medición de riesgos operativos;
d) Monitorear y reportar el perfil de riesgo operativo;
e) Diseñar y brindar capacitación y concientización sobre los riesgos operativos;

3. Tercera línea

a) Revisar el diseño y la implementación de los sistemas de gestión de riesgos operativo y los procesos asociados de la primera y segunda línea de defensa;
b) Revisar los procesos para garantizar que sean independientes y se implementen de manera coherente con las políticas establecidas;
c) Asegurar que los sistemas de cuantificación utilizados para evaluar el riesgo operativo reflejen el perfil de riesgo operativo de la entidad;

ARTÍCULO 5.- Las entidades controladas deben identificar los riesgos operativos por la línea de negocio, tipo de evento, factor de riesgo operativo y las fallas o insuficiencias, utilizando para el efecto, una metodología debidamente documentada y aprobada que incorporará la utilización de

herramientas que se ajusten a las necesidades de la entidad, tales como: autoevaluación, mapas de riesgos, indicadores, tablas de control (scorecards), bases de datos u otras.

Los tipos de eventos de riesgo operativo que deben considerarse, al menos, son los listados a continuación; para un mayor detalle referirse al Anexo No. 1, de la presente norma:

1. Fraude interno
2. Fraude externo
3. Prácticas laborales y seguridad del ambiente de trabajo;
4. Prácticas relacionadas con los clientes, los productos y el negocio;
5. Daños a los activos físicos;
6. Interrupción del negocio por fallas en la tecnología de la información; y,
7. Deficiencias en el diseño y/o la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

ARTÍCULO 6.- Una vez identificados los riesgos operativos y las fallas o insuficiencias en relación con los factores de este riesgo, se debe medir el riesgo determinando su probabilidad de ocurrencia e impacto para la entidad, permitiendo al directorio y a la alta gerencia contar con una visión clara de la exposición al riesgo operativo, con el objetivo de alertarlos en la toma de decisiones y acciones, de manera que el directorio esté en capacidad de decidir si mitiga, transfiere, asume o evita el riesgo reduciendo sus efectos.

Las entidades controladas deben implementar mecanismos de cuantificación periódica sobre los eventos de pérdidas producidos por este tipo de riesgos, que permitan reevaluar la declaración de tolerancia institucional ante el riesgo operativo.

ARTÍCULO 7.- Aspecto importante de la administración del riesgo operativo es el control, el cual requerirá que las entidades controladas cuenten con planes de mitigación formalmente establecidos y validados periódicamente, mediante la revisión de estrategias y políticas; actualización o modificación de procesos y procedimientos establecidos; implementación o modificación de límites de riesgo; implementación o modificación de controles; plan de continuidad del negocio; revisión de términos de pólizas de seguro contratadas; contratación de servicios provistos por terceros; u otros, según corresponda. Los controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron. Las entidades controladas deberán implementar mecanismos efectivos para mitigar los riesgos relacionados a los factores del riesgo operativo, adicionales a los señalados en la presente norma.

ARTÍCULO 8.- Las entidades controladas deben realizar un monitoreo permanente de los riesgos asociados a sus procesos, su nivel de exposición y deben contar con un esquema organizado de reportes e informes que permita tener información suficiente, pertinente y oportuna para la toma de decisiones, el cual debe incluir, como mínimo:

1. Reporte de indicadores claves de riesgo operativo que permitan evaluar la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas;

2. Reporte del grado de cumplimiento de los planes de mitigación;

3. Reporte de la matriz y mapas de riesgos operativos, que incluya, como mínimo: línea de negocio, proceso, subproceso, tipo de riesgo, riesgo / evento de riesgo operativo, factor de riesgo operativo, fallas o insuficiencias, impacto inicial, probabilidad inicial, frecuencia, riesgo inherente/ inicial, controles existentes/ planes de mitigación, impacto final, probabilidad final y riesgo residual.

Además, la entidad controlada en los informes trimestrales dirigidos al comité de administración integral de riesgos, debe incluir los niveles de exposición al riesgo operativo, la evolución de los

riesgos reflejados en sus respectivos indicadores clave de riesgos; la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas; el grado de cumplimiento de los planes de mitigación; y, conclusiones y recomendaciones; de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en la administración del riesgo operativo; así como, para establecer o modificar políticas, procesos, procedimientos y metodologías, entre otros.

ARTÍCULO 9.- En razón de que la administración del riesgo operativo constituye un proceso continuo y permanente; y, para una gestión efectiva del riesgo, las entidades controladas deben conformar bases de datos centralizadas, que permitan registrar, ordenar, clasificar y disponer de información sobre los riesgos y eventos de riesgo operativo incluidos los de orden legal, de seguridad de la información, servicios provistos por terceros y de continuidad del negocio, el efecto cuantitativo de pérdida producida y estimada, así como, la frecuencia y probabilidad, y otra información que las entidades controladas consideren necesaria y oportuna, para que se pueda estimar las pérdidas atribuibles a este tipo de riesgo. La administración de la base de datos es responsabilidad de la unidad de riesgo operativo.

ARTÍCULO 10.- Las entidades controladas deben definir una política de comunicación formal sobre los eventos de riesgo operativo que deban informar interna o externamente y que esté sujeta a revisión periódica, en función de las estrategias organizacionales. Además, deben implementar un proceso para evaluar el impacto de la información a comunicar en función a su gestión de riesgos.

ARTÍCULO 11.- La función de auditoría interna, al encargarse del aseguramiento independiente, es la responsable de evaluar objetiva e independientemente, que las unidades y las actividades de la institución relacionadas con la gestión del riesgo operativo en la primera y segunda línea de defensa, cumplan con los lineamientos establecidos en la presente norma, en concordancia con lo dispuesto en la Norma de Control para la Calificación de los Auditores Internos de las Entidades de los Sectores Financieros Público y Privado de la Codificación de Normas de la Superintendencia de Bancos, en su parte pertinente.
Sin perjuicio de lo mencionado, deberá verificar la eficacia de los controles implementados para mitigar el riesgo operativo en cada uno de sus factores y generar los informes respectivos que evidencien dicha labor, incluyendo:

1. La verificación de la efectividad de las medidas de seguridad que la entidad controlada debe implementar en sus canales electrónicos y/o tarjetas.

2. La revisión periódica de la efectividad del sistema de gestión de continuidad del negocio y del sistema de gestión de la seguridad de la información.

SECCIÓN III.- FACTORES DEL RIESGO OPERATIVO

ARTÍCULO 12.- Con el propósito de minimizar la probabilidad de incurrir en pérdidas atribuibles al riesgo operativo, las entidades controladas deben administrar el riesgo operativo para cada uno de sus factores, que son: procesos, personas, tecnología de la información y eventos externos.

ARTÍCULO 13.-Factor Procesos.- Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las entidades controladas adoptarán un enfoque eficiente y eficaz de gestión por procesos, tomando como referencia el estándar ISO 9001; y, puede incluir, pero no se limita a:

1. Definir el mapa de procesos de conformidad con la estrategia y las políticas adoptadas por la entidad, mismos que deben ser agrupados de la siguiente manera:

a) Procesos gobernantes o estratégicos.- Se considerarán a aquellos que proporcionan directrices y políticas a la organización, cuya responsabilidad compete al directorio y la alta

gerencia para poder cumplir con los objetivos institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, continuidad del negocio, seguridad de la información, entre otros.

b) Procesos productivos, fundamentales u operativos.- Son los procesos esenciales de la entidad, destinados a llevar a cabo las actividades que permiten ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,

c) Procesos habilitantes, de soporte o apoyo.- Son aquellos que permiten a los procesos gobernantes y productivos, su ejecución.

2. Asignar los procesos productivos a las líneas de negocio de acuerdo con los productos y servicios que generan, de forma que, a cada uno de los procesos le corresponda una línea de negocio y que ningún proceso permanezca sin asignar; si algún proceso productivo interviene en más de una línea de negocio, la entidad debe utilizar la metodología que haya establecido formalmente para el efecto.

3. Definir formalmente una metodología para el diseño, control, actualización, seguimiento y medición de los procesos. La metodología debe contener, al menos, pero sin limitarse a, lo siguiente:

a) Descripción y diagramación en secuencia lógica y ordenada de las actividades, tareas, y controles.

b) Determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento; y, del establecimiento de controles y planes de acción para una correcta administración del riesgo operativo. Para el efecto, deberán establecer controles o planes de mitigación que permitan minimizar la ocurrencia de posibles eventos de riesgo y su impacto, garantizando su actualización.

c) Identificación de los clientes internos y externos.

d) Productos y servicios que genera.

e) Difusión y comunicación de los procesos buscando garantizar su correcta aplicación; y,

f) Actualización y mejora continua a través del seguimiento periódico en su aplicación, al menos, una vez al año para los procesos productivos; y, para el resto, al menos, una vez cada dos años.

4. Mantener inventarios actualizados de los procesos existentes, que cuenten, como mínimo, con la siguiente información: Categoría del proceso (gobernante, productivo, de apoyo), línea de negocio, nombre del proceso, tipo de proceso (crítico, no crítico), nombre de procedimientos asociados al proceso, responsables del proceso (nombre, cargo, área), producto o servicio entregado, fecha de aprobación, fecha de actualización.

5. Mantener separación de funciones que evite concentraciones de carácter incompatible, entendidas estas, como aquellas tareas cuya ejecución por una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo.

6. Definir indicadores para cada uno de los procesos que le permitan a la entidad medir la eficacia y eficiencia de éstos.

ARTÍCULO 14.- Factor Personas.- Las entidades controladas deben administrar el capital humano de forma que les permita gestionar los riesgos asociados a este factor.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las entidades controladas deben:

1. Definir formalmente políticas, procesos y procedimientos para la incorporación, permanencia y desvinculación del personal al servicio de la entidad, soportados técnicamente y ajustados a las disposiciones legales, de manera que, aseguren la planificación y administración del capital humano, mismos que corresponden a:

a) Incorporación.- Comprende la planificación de necesidades, el reclutamiento y la selección, la contratación e inducción de nuevo personal. Las entidades controladas deben evaluar su organización con el objeto de definir el personal mínimo necesario, la modalidad de trabajo y las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.

b) Permanencia.- Comprende la creación de condiciones laborales idóneas mediante la planificación y ejecución de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; un sistema de evaluación del desempeño que permita medir y estimular la gestión del personal de la entidad y a su vez aplicar incentivos que motiven la adhesión a los valores institucionales; identificar los puestos críticos y el personal clave de la entidad y definir el personal de reemplazo en el caso de ausencia temporal o definitiva, con la finalidad de dar continuidad a las operaciones del negocio.

c) Desvinculación.- Comprende la planificación de la salida del personal por causas regulares o irregulares a través de la preparación de aspectos jurídicos para llegar al finiquito y a la finalización de la relación laboral.

2. La entidad controlada debe asegurar que se mantengan actualizados los acuerdos de confidencialidad relacionados con los procesos que ejecuta el empleado y los riesgos asociados a las funciones que desempeña.

3. La entidad controlada debe determinar responsabilidades y deberes de seguridad de la información que permanezcan vigentes después del cambio de funciones o de la terminación de la relación laboral, mismos que deben ser incluidos en el acuerdo de confidencialidad.

4. Mantener un archivo digital centralizado con información actualizada del capital humano, misma que deberá detallar: formación académica y experiencia; forma y fechas de reclutamiento, selección y contratación; información histórica sobre los eventos de capacitación en los que ha participado; cargos que ha desempeñado en la entidad; resultados de evaluaciones de desempeño realizadas; fechas y causas de separación del personal que se ha desvinculado; con la finalidad de permitir la toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades.

ARTÍCULO 15.- Factor Tecnología de la Información.- Las entidades controladas deben contar con tecnología de la información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna, confiable y segura; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, esté disponible para la toma de decisiones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo tecnológico, las entidades controladas deben, como mínimo, pero sin limitarse a:

1. Contar con un área de tecnología de la información en función del tamaño y complejidad de las operaciones, y conformar el comité de tecnología, que es el responsable de evaluar, y supervisar las actividades estratégicas de carácter tecnológico.

El comité de tecnología estará integrado como mínimo por: un miembro del directorio, quien lo presidirá, el representante legal de la entidad, el funcionario responsable del área de riesgo operativo, el funcionario responsable del área de seguridad de la información y el funcionario responsable del área de tecnología, quienes no podrán delegar su participación; a excepción del representante legal, que podrá efectuar esta delegación solamente a quien le subrogue estatutariamente en sus funciones. En caso de ausencia temporal o definitiva del miembro del directorio de la entidad del sector financiero público, el comité será presidido por el representante legal, en cuyo caso esta presidencia no será delegable.

El comité de tecnología expedirá un reglamento en donde se establezcan, como mínimo, el objetivo, sus funciones y responsabilidades, que será aprobado conforme corresponda dentro de la estructura organizacional de la entidad controlada.

Las reuniones de este comité se realizarán, al menos, trimestralmente o cuando la situación lo amerite, dejando evidencia de las decisiones adoptadas, mismas que deben ser comunicadas al Directorio.

2. Con el objeto de garantizar que la administración de la tecnología de la información soporte los requerimientos de operación actuales y futuros de la entidad, esta debe contar, al menos, con lo siguiente, pero sin limitarse a ello:

a) El apoyo y compromiso formal del directorio, a través de la aprobación de un plan estratégico de tecnología de la información alineado con el plan estratégico institucional; y, un plan operativo anual que establezca las actividades a ejecutar en el corto plazo, traducido en tareas, cronogramas, personal responsable y presupuesto, de manera que se asegure el logro de los objetivos tecnológicos propuestos; y,

b) Políticas, procesos, procedimientos y metodologías de tecnología de la información, alineados a los objetivos y actividades de la entidad, así como las consecuencias de su incumplimiento.

Las políticas, procesos, procedimientos y metodologías de tecnología de la información deben ser revisados y aceptados por el comité de tecnología y propuestos para la posterior aprobación del directorio; deben ser difundidos y comunicados a todo el personal involucrado de tal forma que se asegure su cumplimiento.

La aprobación de los manuales de procesos, procedimientos y metodologías de tecnología de la información podrá ser delegada al comité de tecnología de la información; y en estos casos debe poner en conocimiento del Directorio lo aprobado por dicho Comité.

3. Con el objeto de garantizar que las operaciones de tecnología de la información satisfagan los requerimientos de las entidades controladas, se debe implementar, al menos, lo siguiente, pero sin limitarse a ello:

a) Procedimientos que establezcan las actividades y responsables de la operación y el uso de los centros de datos, que incluyan controles que eviten accesos no autorizados;

b) Procedimientos de gestión de incidentes y problemas de tecnología de la información, que considere al menos: el análisis de la causa raíz del problema con personal técnico independiente del personal que administra y opera las plataformas afectadas por los incidentes; mantener una base de conocimiento y errores conocidos; definición e implementación de planes de acción efectivos que les permita mitigar la recurrencia así como la correlación de eventos e incidentes catalogados como problemas; implementación de técnicas de gestión de problemas de TI de acuerdo a la naturaleza, tamaño y complejidad de la entidad controlada; y definición e implementación de indicadores clave de rendimiento para la gestión de problemas de TI.

c) Procedimientos de respaldo de información periódicos, acorde a los requerimientos legales y de continuidad del negocio, que incluyan: la frecuencia de verificación, eliminación y el transporte seguro hacia una ubicación remota, que no debe estar expuesta a los mismos riesgos del sitio principal y mantenga las condiciones físicas y ambientales necesarias para su preservación y posterior recuperación.

4. Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las entidades controladas deben implementar una metodología que permita la administración y control del ciclo de vida de desarrollo y mantenimiento de las aplicaciones informáticas, acorde a las mejores prácticas internacionales; y, que, en función de su naturaleza, considere aspectos como los siguientes, pero sin limitarse a ellos:

a) Requerimientos funcionales aprobados por el área solicitante;

b) Requerimientos técnicos y el análisis de la relación y afectación a la capacidad de la infraestructura tecnológica actual, aprobados por el área técnica;

c) Técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones informáticas, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades;

d) Levantamiento y actualización de la documentación técnica y de usuario de las aplicaciones informáticas de la entidad;

e) Aseguramiento de la calidad de software que incluya pruebas técnicas y funcionales que reflejen la aceptación de los usuarios autorizados, así como la verificación del cumplimiento de estándares de desarrollo definidos por la entidad, aspectos que deben ser ejecutados por personal independiente al área de desarrollo y mantenimiento de software;

f) Controles para el paso a producción y versionamiento de las aplicaciones informáticas, que considere su registro y autorizaciones respectivas e incluya los cambios emergentes;

g) Seguimiento postproducción que permita verificar que el sistema puesto en producción funciona de manera estable;

h) Para los casos de migración de información, la entidad debe determinar y aplicar controles para garantizar las características de integridad, disponibilidad y confidencialidad; y,

i) En caso de que la entidad controlada contrate el servicio de desarrollo de software o adquiera un sistema informático, debe verificar que el proveedor cumple con las disposiciones descritas en los numerales precedentes.

5. Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada, las entidades controladas deben implementar, al menos, lo siguiente, pero sin limitarse a:

a) Infraestructura que soporta los procesos críticos con la redundancia necesaria para evitar puntos únicos de falla; de la cual se debe mantener el inventario y respaldos de la configuración actualizada e informes de su mantenimiento periódico; en el caso de los enlaces de comunicación, debe considerar que la trayectoria de los enlaces principal y alterno sean diferentes;

b) Procedimientos que permitan la administración y monitoreo de las bases de datos, redes de datos, hardware y software base, que incluya límites y alertas;

c) Un informe de análisis de la capacidad y desempeño de la infraestructura tecnológica, incluyendo entre otros aspectos, recursos y capacidad dinámica para adaptarse a demandas variables para los servicios de infraestructura, que soporten las operaciones del negocio, que debe ser conocido y analizado por el comité de tecnología con una frecuencia mínima semestral. El informe debe proporcionar a la entidad controlada información técnica sobre las necesidades de actualización de la infraestructura tecnológica por obsolescencia de acuerdo con un proceso de madurez tecnológica, que le permita soportar las operaciones críticas del negocio, además, debe incluir las alertas que hayan sobrepasado los límites de operación segura, dentro de la plataforma tecnológica, al menos, para: almacenamiento, memoria, procesador, consumo de ancho de banda; y, para bases de datos: memoria, procesamiento, áreas temporales de trabajo, log de transacciones, almacenamiento de datos, entre otras;

d) Para los casos de migración de la plataforma tecnológica crítica, controles para gestionar la continuidad del servicio, previa notificación con, al menos, 21 días de anticipación;

e) Centros de procesamiento de datos, principal y alterno, en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado, daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida; y, condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de la información. La ubicación del centro de procesamiento de datos alterno no debe estar expuesta a los mismos riesgos del sitio principal;

f) Ambientes aislados con la debida segregación de accesos para desarrollo, pruebas y producción, los cuales deben contar con la capacidad requerida para cumplir sus objetivos. Al menos, se debe contar con dos ambientes: desarrollo y producción; y,

g) Para el caso de infraestructura provista por terceros, asegurar el cumplimiento de las disposiciones incluidas en los numerales precedentes.

6. Con la finalidad de asegurar que los cambios a los aplicativos e infraestructura que soportan las operaciones estén debidamente autorizados, documentados, probados, y aprobados por el propietario de la información previo a su paso a producción, las entidades controladas deben implementar procedimientos de control de cambios, acorde a las metodologías y mejores prácticas nacionales e internacionales de la industria, que considere aspectos como los siguientes, pero sin limitarse a:

a) Mecanismos mediante los cuales se iniciarán las solicitudes de cambio;

b) Una metodología para analizar, dar prioridad y aprobar las solicitudes de cambio;

c) Evaluación del impacto de los cambios sobre los aplicativos e infraestructura de producción;

d) Mecanismos de marcha atrás, de modo que el impacto por cualquier falla pueda ser minimizado;

e) Librerías de desarrollo separadas de las librerías de producción, para evitar que una versión de prueba pueda contener código no autorizado;

f) Mecanismos que aseguren que los cambios a los aplicativos y a su documentación, se realizan sobre las versiones fuente de los elementos en producción, y que los cambios realizados al código de las aplicaciones informáticas corresponden a aquellos solicitados por el propietario de la información;

g) El responsable de aseguramiento de la calidad supervisa el mantenimiento de versiones de programa, código fuente o registros de configuración de la infraestructura, para garantizar su integridad;

h) El responsable del aseguramiento de la calidad debe realizar, en ambientes no productivos, junto con el propietario de información, las pruebas y certificación sobre los cambios para garantizar que: ejecuten las funciones requeridas, que la funcionalidad y desempeño existente no se vean afectadas por el cambio, que no se hayan generado riesgos de seguridad debido al cambio y que se cuente con toda la documentación actualizada; una vez concluidas exitosamente las pruebas, se debe registrar la aprobación del cambio;

i) Mecanismos para garantizar que el paso de programas desde el ambiente de desarrollo a pruebas y de producción, sea realizado por un grupo independiente a los programadores; y,

j) Procedimientos de cambios de emergencia para casos excepcionales en donde no sea posible seguir el proceso completo de control de cambios que incluya su posterior regularización y que permitan asegurar que no se compromete la integridad del sistema e infraestructura.

ARTÍCULO 16.- Eventos Externos.- En la administración del riesgo operativo, las entidades controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, ataques cibernéticos, eventos de conmoción social, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades.

La gestión de los riesgos relacionados con eventos externos debe formar parte de la administración de la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio.

SECCIÓN IV. GESTIÓN DE INCIDENTES Y PROBLEMAS

ARTÍCULO 17.- Las entidades controladas deben desarrollar e implementar planes de respuesta y recuperación para gestionar los incidentes y problemas que puedan afectar el normal funcionamiento de sus servicios, especialmente, de sus servicios críticos en línea con el apetito y la tolerancia al riesgo definida por la entidad, de manera que contribuya a la resiliencia operativa de la entidad; para lo cual, las entidades controladas deben garantizar la disponibilidad de los servicios críticos que se ofrecen a los usuarios financieros en un 99.99% anual; y, mantener lo siguiente pero sin limitarse a:

1. Asignar un gestor de incidentes y problemas, quien deberá encargarse de la trazabilidad hasta finalizar la atención de los incidentes y problemas; y, su respectivo registro en la base de conocimiento.

2. Establecer políticas, procesos, procedimientos y metodologías para la gestión de incidentes y de problemas, que puedan afectar a los factores de riesgo operativo.

3. La gestión de incidentes debe abarcar el ciclo de vida del incidente, que incluya entre otros: registro, priorización en función de la gravedad, análisis, escalamiento, solución, monitoreo, lecciones aprendidas y reporte a las partes interesadas tanto internas como externas.

4. La gestión de problemas debe considerar al menos: el análisis de la causa raíz del problema con personal técnico independiente del personal que administra y opera las plataformas afectadas por los incidentes; y, mantener una base de conocimiento y errores conocidos; definición e implementación de planes de acción efectivos que les permita mitigar la recurrencia, así como la correlación de eventos e incidentes catalogados como problemas.

5. Ejecutar pruebas controladas de gestión de incidentes y problemas.

6. Mantener una base de conocimiento de respuesta a incidentes y recuperación que incluya recursos internos y de terceros, según aplique, para respaldar las capacidades de respuesta y

reanudación de los servicios. Los procedimientos asociados deben revisarse, probarse y actualizarse periódicamente por las áreas involucradas;

7. Las entidades controladas deben comunicar a la Superintendencia de Bancos los incidentes que afecten a sus servicios críticos, al correo electrónico definido para el efecto conforme a las disposiciones y circulares emitidas por el organismo de control, y remitir un informe formal del incidente máximo en los 5 días plazo siguientes al incidente; y, en 20 días plazo el informe de causa raíz del problema.

8. Las entidades controladas deben aplicar los planes de contingencia y continuidad del negocio cuando los incidentes afecten a sus servicios críticos conforme a la evaluación del impacto del incidente.

SECCIÓN V. GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

ARTÍCULO 18.- Administración de la Continuidad del Negocio.- Las entidades controladas deben establecer, implementar, mantener y mejorar un sistema de gestión de la continuidad del negocio, para garantizar su capacidad de operar de forma continua y limitar las pérdidas en caso de una interrupción grave del negocio, tomando como referencia los estándares de la serie ISO 22301, o el que lo sustituya; mismo que debe contemplar eventos internos y externos, así como, las estrategias para la continuidad del negocio, de manera que contribuya a la resiliencia operativa de la entidad; por lo cual, debe contar con, al menos, con lo siguiente, pero sin limitarse a estos:

1. Un comité de continuidad del negocio que esté conformado como mínimo por los siguientes miembros: un miembro del directorio, quien lo presidirá, el representante legal de la entidad, los funcionarios responsables de las unidades de: riesgos, tecnología de la información, seguridad de la información, talento humano, y, el responsable de la continuidad del negocio quien actuará como secretario. Los representantes de cada una de las áreas relacionadas con los procesos críticos de la entidad y auditoría interna participarán con voz sin voto. El representante legal podrá delegar su participación solamente a quien le subrogue estatutariamente en sus funciones. En caso de ausencia temporal o definitiva del miembro del directorio de la entidad del sector financiero público, el comité será presidido por el representante legal, en cuyo caso esta presidencia no será delegable.

El comité de continuidad del negocio expedirá un reglamento en donde se establezcan, como mínimo, el objetivo, sus funciones y responsabilidades. Las reuniones de este comité se realizarán, al menos, trimestralmente, o cuando se las requiera.

El comité de continuidad del negocio debe dejar evidencia de las decisiones adoptadas, las cuales deben ser conocidas y aprobadas por el comité de administración integral de riesgos.

El comité de continuidad del negocio debe tener, al menos, las siguientes responsabilidades, pero sin limitarse a:

a) Evaluar y supervisar el sistema de gestión de continuidad del negocio;

b) Monitorear la implementación del plan de continuidad del negocio y asegurar el alineamiento de este con la metodología de administración de la continuidad del negocio;

c) Proponer para la revisión y aceptación del comité de administración integral de riesgos, el plan de continuidad del negocio y sus actualizaciones;

d) Revisar el presupuesto del plan de continuidad del negocio y ponerlo en conocimiento del comité de administración integral de riesgos;

e) Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; y,

f) Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad del negocio.

2. La entidad debe contar con una persona o área responsable de la gestión de la continuidad de negocio, acorde al tamaño y complejidad de la entidad, que dirija el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de continuidad del negocio de la entidad. El responsable debe tener la capacitación o formación, y experiencia en el ramo.

ARTÍCULO 19.- El marco de referencia del sistema de gestión de continuidad del negocio debe contener, al menos, lo siguiente, pero sin limitarse a:

1. Alcance del sistema de gestión de continuidad en términos del negocio que considere los procesos críticos.

2. Políticas, estrategias, objetivos, procesos, procedimientos, metodologías, planes y presupuesto para la administración de la continuidad del negocio, que deben ser revisados y actualizados al menos 1 vez al año o cuando existan cambios significativos; y, aceptados por el comité de continuidad del negocio; y, propuestos por el comité de administración integral de riesgos, para la posterior aprobación del directorio. Esta documentación debe ser difundida y comunicada a todo el personal involucrado, de tal forma que se asegure su cumplimiento.

3. Funciones y responsables de las actividades de continuidad de las operaciones, que permitan cumplir con el criterio de resiliencia para la disponibilidad de las operaciones, acorde al tamaño y complejidad de los procesos administrados por el negocio.

4. Análisis de impacto del negocio (BIA) que tendría una interrupción de los procesos que soportan los productos y servicios de la entidad. Para ello, deben aplicar los parámetros para la identificación de los procesos críticos, su punto de recuperación objetivo (RPO) y tiempos de recuperación objetivo (RTO) definidos por el negocio, los cuales debe ser revisados y de ser el caso actualizados al menos 1 vez al año; una vez identificados los procesos críticos, deben determinar las dependencias internas y externas; y, recursos de soporte para estos procesos, incluyendo tecnología, personal, proveedores y otras partes interesadas. Los RPO y RTO de sus proveedores externos deben cumplir cuando menos con los valores de estos definidos por la entidad para sus procesos críticos.

El análisis de impacto del negocio (BIA) debe ser revisado al menos 1 vez al año y/o actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados.

5. Identificación de los principales escenarios de riesgos, incluyendo las fallas en la tecnología de la información, tomando en cuenta el impacto y la probabilidad de que sucedan. Para ello, debe seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos.

6. Definición, evaluación y selección de estrategias de continuidad por cada proceso crítico que permitan mantener su operatividad, dentro del tiempo objetivo de recuperación definido para cada proceso, mismas que deben tomar en cuenta, al menos, lo siguiente: la seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas de trabajo, infraestructura alterna de procesamiento, información necesaria para el proceso; proveedores y aplicativos relacionados.

7. Planes de contingencia y de continuidad del negocio que permita asegurar la disponibilidad de los productos y servicios críticos de la entidad controlada y disminuir los efectos de eventos disruptivos.

8. Procedimientos de pruebas de los planes de contingencia y del plan de continuidad del negocio que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o, al menos, una vez al año; las pruebas deben incluir el alcance y el detalle de los aspectos a probar, incluida la participación de los proveedores, así como las conclusiones y recomendaciones obtenidas como resultado de su ejecución.

La entidad controlada periódicamente debe monitorear y evaluar el servicio prestado; así como verificar que auditoría interna o su equivalente del proveedor de servicios asegure que los planes de contingencia y/o continuidad de las compañías contratadas que soportan los servicios críticos de la entidad se encuentren actualizados, y que estos sean debidamente probados con la intención de precautelar los servicios brindados. Además, la entidad controlada debe incluirlos dentro de sus pruebas anuales de continuidad y el resultado de estas debe ser comunicado a las instancias correspondientes.

9. Procedimientos para monitorear, medir y evaluar el desempeño y eficacia del sistema de gestión de la continuidad del negocio.

10. Procedimientos de difusión, comunicación, entrenamiento y concienciación de los planes de contingencia y plan de continuidad del negocio.

11. Incorporación del proceso de administración de la continuidad del negocio al proceso de administración integral de riesgos, que garantice la actualización y mejora continua del plan de continuidad del negocio.

12. La entidad debe mantener una base de conocimiento de las lecciones aprendidas en función del resultado de las pruebas realizadas al plan de continuidad del negocio, eventos de continuidad materializados, debilidades encontradas en las revisiones efectuadas por la administración de la continuidad del negocio, entre otros.

ARTÍCULO 20.- Plan de Continuidad del Negocio.- Las entidades controladas deben contar con un plan de continuidad del negocio, cuya estructura considere como mínimo lo siguiente, pero sin limitarse a:

1. Escenarios de riesgos y procesos críticos cubiertos por el plan;

2. Tiempo de recuperación objetivo (RTO) y punto de recuperación objetivo (RPO) de cada proceso crítico, conforme lo identificado en el análisis de impacto en el negocio;

3. Estrategias de continuidad por cada proceso crítico con el detalle de, al menos, lo siguiente, pero sin limitarse a: el personal asociado, instalaciones alternas de trabajo, infraestructura alterna de procesamiento, proveedores, aplicativos relacionados, información vital de acuerdo con el análisis de la entidad y cómo acceder a ella;

4. Procedimientos operativos que incluyan las acciones para trasladar las actividades de la entidad controlada a ubicaciones transitorias alternativas y para restablecer los procesos críticos de manera urgente; para lo cual deben establecer un centro alterno de operaciones que no esté expuesto a los mismos riesgos del sitio principal;

5. Procedimientos de comunicaciones que incluyan: las estrategias de comunicación con el personal involucrado, sus familiares y contactos de emergencia, con información tal como: direcciones, teléfonos, correos electrónicos, entre otros; interacción con los medios de comunicación; y, comunicación con los grupos de interés;

6. Procedimientos de emergencias que describan las acciones a ejecutar para preservar la seguridad del personal;

7. Plan de recuperación de desastres que detalle los procedimientos tecnológicos de restauración en una ubicación remota de los servicios de tecnología de la información, mismos que deben estar dentro de los parámetros establecidos en el plan de continuidad del negocio, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. La ubicación remota no debe estar expuesta a los mismos riesgos del sitio principal;

8. Roles y responsabilidades de las personas encargadas de ejecutar cada actividad en los procedimientos operativos, de comunicaciones, de emergencia, plan de recuperación de desastres y aspectos logísticos;

9. Criterios de invocación y activación del plan de continuidad del negocio; y,

10. Las entidades que tengan dependencia tecnológica y/u operativa con su matriz en el exterior deben tener su plan de continuidad local, conforme la presente norma, y deberá estar correlacionado con las estrategias del plan de continuidad de su casa matriz.

SECCIÓN VI.- RIESGO LEGAL

ARTÍCULO 21.- Con la finalidad de gestionar el riesgo legal y minimizar la probabilidad de incurrir en pérdidas por este tipo de riesgo, las entidades controladas deben identificar, medir, controlar, mitigar y monitorear los eventos que podrían ocasionar la materialización del riesgo legal de acuerdo con su propia percepción y perfil de riesgos, orientándolos pero sin limitarse a: los actos societarios, la gestión de crédito, las operaciones del giro financiero, las actividades complementarias a las del objeto social, empresas proveedoras nacionales y extranjeras, estipulaciones contractuales y, cumplimiento legal y normativo.

ARTÍCULO 22.- Las entidades controladas, en función de su tamaño y complejidad de operaciones, mantendrán un área de asesoría jurídica - legal con nivel de reporte a la gerencia general, con atribuciones y funciones formales para gestionar el riesgo legal; y, contarán con personal capacitado y experimentado. La citada área como parte de sus funciones, mantendrá matrices de gestión de riesgos legales a los que pudieran estar expuesta la entidad controlada.

SECCIÓN VII.- SERVICIOS PROVISTOS POR TERCEROS

ARTÍCULO 23.- Para mantener el control de los servicios provistos por terceros, incluidas las empresas de servicios auxiliares del sistema financiero, las entidades controladas deben implementar un proceso integral para la administración de proveedores de servicios que incluya las actividades previas a la contratación, suscripción, cumplimiento y renovación del contrato; para lo cual, deben cumplir, por lo menos, con lo siguiente, pero sin limitarse a:

1. Para las actividades previas a la contratación, las entidades controladas deben establecer e implementar políticas, procesos y procedimientos que aseguren la evaluación, calificación y selección de los proveedores, relacionados con y sin limitarse a:

a) Evaluación de la experiencia de la empresa y de su personal;

b) Evaluación financiera para asegurar la viabilidad de la empresa durante todo el período de contratación previsto;

c) Análisis de informes de auditoría externa, si los tuviere;

d) Evaluación de la capacidad del servicio, instalación y soporte e historial del desempeño con base en los requisitos de la entidad controlada;
e) Evaluación de la capacidad logística de la empresa, incluyendo la infraestructura física y tecnológica y recursos humanos;

f) Análisis del riesgo reputacional de la empresa; y,

g) Gestión de riesgos asociados a los servicios críticos provistos por terceros, que garanticen la gestión de seguridad de la información incluyendo ciberseguridad y la gestión de la continuidad del negocio, en función a la naturaleza del servicio contratado.

2. Establecer políticas, procesos y procedimientos que aseguren la contratación de servicios en función de los requerimientos de la entidad controlada, y garanticen que los contratos incluyan, como mínimo, las siguientes cláusulas:

a) Niveles mínimos de calidad del servicio acordado.

b) Garantías financieras y técnicas, tales como: buen uso del anticipo, fiel cumplimiento del contrato, buen funcionamiento y disponibilidad del servicio, entre otros.

c) Multas y penalizaciones por incumplimiento.

d) Personal suficiente y calificado para brindar el servicio en los niveles acordados.

e) Capacitación, en los casos que aplique, del servicio contratado y entrega de toda la documentación que soporta el proceso o servicio asociado a los procesos críticos.

f) Seguridad de la información incluyendo Ciberseguridad y protección de datos personales sobre la gestión de información usada de la entidad controlada en la provisión del servicio proporcionado por el proveedor.

g) Derechos de propiedad intelectual, cuando aplique.

h) Definición del equipo de contraparte y administrador del contrato tanto de la entidad controlada como del proveedor.

i) Definición detallada de los productos y servicios a ser entregados por el proveedor.

j) Cumplimiento por parte del proveedor de las políticas que establezca la entidad controlada, las cuales deben incluir, al menos, la norma expedida por la Superintendencia de Bancos, aplicable en función del servicio a ser contratado.

k) Facilidades para la revisión y seguimiento del servicio prestado a las entidades controladas, por parte de la unidad de auditoría interna u otra área que estas designen, así como de los auditores externos y la Superintendencia de Bancos, en aquellos procesos definidos como críticos.

l) Informes de auditoría externa sobre el cumplimiento de los aspectos relacionados con la seguridad de la información y continuidad del negocio referidos en la presente norma, practicados por personal o empresas independientes con experiencia acreditada en el ramo emitidos en el último año; o, certificaciones en temas de Seguridad de la Información incluida ciberseguridad y continuidad del negocio, vigentes obtenidas ante certificadoras acreditadas, el alcance de los informes o certificaciones debe ser aplicable al servicio contratado.

3. Administrar los riesgos a los que se exponen al contratar servicios provistos por terceros, particularmente de aquellos que soportan los procesos críticos.

4. Establecer políticas, procesos y procedimientos que aseguren el control y monitoreo de los servicios contratados, mediante la evaluación, gestión y vigilancia de éstos, a fin de garantizar que se cumplan en todo momento con los niveles mínimos de servicio acordados y demás cláusulas establecidas en el contrato. La información utilizada para el monitoreo de los servicios contratados debe ser obtenida por la entidad controlada de manera independiente de aquella

que proporcione el proveedor, para lo cual podrá utilizar los mecanismos técnicos que considere pertinentes, que le permita confirmar el cumplimiento de las condiciones contractuales.

5. Contar con proveedores alternos de los servicios que soportan a los procesos críticos, que tengan la capacidad de prestar el servicio para mitigar el riesgo de dependencia en un solo proveedor; en los casos de proveedor único, la entidad controlada debe asegurarse de que el proveedor cuenta con planes de contingencia y continuidad de negocio, que han sido probados y se encuentran actualizados, al menos, anualmente y sincronizados con los tiempos definidos por el banco.

6. Para el caso de contratación de servicios de infraestructura, plataforma y/o software, en la nube tanto con proveedores nacionales o extranjeros; las entidades controladas deberán disponer conforme el servicio contratado: Un informe técnico, uno de seguridad de la información y uno legal, emitido por el personal de la entidad controlada en función de sus competencias, en los cuales, se haya identificado los riesgos operativos asociados al servicio y la gestión respectiva.

Además, de identificar y gestionar los riesgos asociados a estos servicios la entidad debe:

a) Informar a la Superintendencia de Bancos sobre el detalle de los servicios asociados a los procesos críticos a ser contratados que incluya entre otros: el tipo de servicio contratado, el detalle del servicio alojado, la arquitectura tecnológica contratada, según aplique; el análisis de los riesgos operativos, legales, tecnológicos, de seguridad de la información incluida la ciberseguridad y continuidad de operaciones a los que se exponen al adoptar este servicio; así como los controles para mitigarlos;

b) Los centros de procesamiento de datos principal y/o alterno, contratados en la nube tanto con proveedores nacionales o extranjeros, deben haber sido implementados siguiendo el estándar ANSI-TIA-942 o superior y contar como mínimo con la certificación TIER III o su equivalente para diseño, implementación y operación y así garantizar la disponibilidad de los servicios brindados;

c) El proveedor de servicios en la nube tanto con proveedores nacionales o extranjeros, debe contar, para los servicios ofertados, como mínimo, con certificación ISO 27001 en seguridad de la información, así como, la implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube), ISO 27018 (protección de información personal en la nube) u otras similares que aplique conforme el servicio ofertado;

7. Si los servicios provistos por terceros son de carácter financiero, estos están sujetos al cumplimiento de la normativa que emita la Junta de Política y Regulación Financiera y la Superintendencia de Bancos, en lo que corresponda.

8. Para los casos en que las entidades financieras contraten la adquisición o acceso a bases de datos con información de personas naturales o jurídicas o de otra naturaleza, deberán aplicar procedimientos para asegurarse que el origen de la información es lícito; y se encuentra acorde con las leyes vigentes en el país.

9. Para la contratación total o parcial de servicios para ejecución de los procesos críticos, en el exterior, las entidades controladas deben notificar a la Superintendencia de Bancos, adjuntando la documentación de respaldo que asegure el cumplimiento de esta sección conforme la naturaleza del servicio contratado.

10. Para los casos en que las entidades financieras contraten servicios con las sociedades especializadas de depósitos y pagos electrónicos (SEDPES); y, con las administradoras de Sistemas Auxiliares de Pago (ASAP); deben garantizar que estas den cumplimiento según corresponda de la presente Norma.

11.La Superintendencia de Bancos definirá los proveedores sistémicos en función de los servicios que ofrezcan y la cobertura que mantengan en las entidades controladas. El detalle de los proveedores sistémicos será puesto en conocimiento de las entidades controladas a fin de que esta característica sea considerada dentro de la gestión integral de sus proveedores.

SECCIÓN VIII.- SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 24.- Con el objeto de gestionar la seguridad de la información, para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las entidades controladas deben tener como referencia la serie de estándares ISO/IEC 27000, otras normas internacionales aplicables en materia de ciberseguridad o las que las sustituyan, y cumplir con las disposiciones legales y normativas vigentes en el país en esta materia; por lo cual, debe contar, al menos, con lo siguiente pero sin limitarse a:

1. Funciones y responsables de las actividades de la seguridad de la información que incluya ciberseguridad, deben estar claramente definidas, que permitan establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información, acorde al tamaño y complejidad de la entidad.

2. Un comité de seguridad de la información que se encargue de evaluar y supervisar el sistema de gestión de seguridad de la información.

El comité debe estar conformado como mínimo por: el miembro del directorio quien lo presidirá, el representante legal de la entidad, los funcionarios responsables de las áreas de: riesgos, tecnología de la información y seguridad de la información, quienes no podrán delegar su participación; a excepción del representante legal, quien podrá delegar su participación solamente a quien le subrogue estatutariamente en sus funciones. En caso de ausencia temporal o definitiva del miembro del directorio de la entidad del sector financiero público, el comité será presidido por el representante legal, en cuyo caso esta presidencia no será delegable.

El comité de seguridad de la información expedirá un reglamento en donde se establezcan, como mínimo, el objetivo, sus funciones y responsabilidades. Las reuniones de este comité se realizarán, al menos, trimestralmente, o cuando la situación lo amerite, dejando evidencia de las decisiones adoptadas. El comité de seguridad de la información reportará directamente al Directorio y mantendrá informado permanentemente a la alta gerencia y al comité de administración integral de riesgos.

3. Un área independiente y especializada de Seguridad de la Información que reporte a la máxima autoridad gerencial de la institución, con personal formado y experiencia en gestión de seguridad de la información y ciberseguridad, acorde al tamaño y complejidad de sus operaciones, que defina estrategias y objetivos de seguridad de la información alineados a las estrategias y objetivos institucionales, que lidere el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información de la entidad; y, que debe mantener la independencia funcional de las áreas del negocio, tecnología, riesgos y función de auditoría.

4. Un responsable del área de seguridad de la información.

ARTÍCULO 25.- Las entidades controladas deben establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información que incluya, al menos, lo siguiente, pero sin limitarse a:

1. Alcance del sistema de gestión de seguridad de la información.

2. Políticas, procesos, procedimientos y metodologías de seguridad de la información que incluya aspectos de ciberseguridad, definidos bajo estándares de general aceptación, alineados a los

objetivos y actividades de la entidad, así como las consecuencias de su incumplimiento. Las políticas, procesos, procedimientos y metodologías de seguridad de la información incluido ciberseguridad, deben ser revisados al menos, una (1) vez al año o cuando se producen cambios significativos; y aceptados por el Comité de seguridad de la información; y, propuestos para la posterior aprobación del Directorio; así como, ser difundidos y comunicados a todo el personal involucrado de tal forma que se asegure su cumplimiento.

La aprobación de los manuales de procesos, procedimientos y metodologías de seguridad de la información y ciberseguridad podrá ser delegada al Comité de Seguridad de la Información, y en estos casos debe poner en conocimiento del Directorio lo aprobado por dicho Comité.

La entidad controlada debe asegurar que sus empleados cumplan con lo establecido en el sistema de seguridad de la información, así como, proporcionar la capacitación y actualizaciones periódicas relacionadas con el mismo.

3. Inventario de activos de la información acorde al alcance del sistema de gestión de seguridad de la información con al menos, su clasificación en términos de: valor, requerimientos legales, sensibilidad y criticidad para la entidad, propietario, custodio y ubicación.

4. La designación de los propietarios de los activos de información, que deben tener como mínimo las siguientes responsabilidades:

a) Clasificar los activos de información y revisar periódicamente el inventario de activos de información, con la finalidad de mantenerlo actualizado.

b) Definir y revisar periódicamente las restricciones para el uso aceptable de la información y accesos a los activos de información, tomando en cuenta las políticas de control de acceso aplicables; y,

c) Autorizar los cambios funcionales a las aplicaciones informáticas y modificaciones a la información a través de accesos directos a la base de datos.

5. La gestión de riesgos de seguridad de la información incluidos los de ciberseguridad, se debe realizar mediante una metodología que le permita identificar, medir, controlar/mitigar y monitorear los riesgos asociados a los activos de información para preservar su confidencialidad, integridad y disponibilidad; esta metodología debe estar alineada a la metodología de gestión del riesgo operativo de la entidad.

6. Plan de seguridad de la información que permita la implementación de los controles identificados y acciones de mejora para mitigar los riesgos de seguridad de la información y ciberseguridad. Para el caso de los controles de seguridad de la información relacionados con aspectos tecnológicos, estos deben responder a soluciones implementables a través de infraestructuras y plataformas que respondan a la arquitectura tecnológica definida por el área de Tecnología de la Información, conforme a las necesidades del negocio.

7. Monitoreo, con una frecuencia al menos semestral del cumplimiento y efectividad de los controles establecidos, dejando evidencia del monitoreo en informes que serán comunicados al Comité de Seguridad de la Información y al Directorio.

8. Evaluación, al menos, una vez al año del desempeño del sistema de gestión de la seguridad de la información, considerando los resultados de: auditorías de seguridad, gestión de incidentes de seguridad, monitoreo de los controles, resultados de las evaluaciones de riesgos, sugerencias, retroalimentación de las partes interesadas, entre otros aspectos; a fin de tomar acciones orientadas a mejorarlo. El resultado de estas evaluaciones, así como las acciones de mejora deben ser conocidas y aprobadas por el comité de seguridad de la información.

9. Para considerar la existencia de un apropiado ambiente de gestión de seguridad de la información, la unidad responsable debe establecer, implementar y controlar, al menos, lo siguiente, pero sin limitarse a:

a) Procedimientos para la clasificación de los activos de la información.

b) Medidas para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización, divulgación no autorizada de información, traslados, entre otros, para fines contrarios a los intereses de la entidad, por parte de su personal o de terceros.

c) Procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios. Además, se deberá controlar la eliminación de la información crítica en las bases de datos o repositorios de los proveedores de la entidad después de que presten sus servicios.

d) Procedimientos para el control de accesos a la información que considere la concesión; administración de usuarios y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como, la revocación de usuarios, tanto de aplicativos, software base, red, dispositivos de seguridad perimetral, bases de datos, entre otros. También se deberá controlar el acceso de los proveedores a la información de la entidad, durante la prestación de sus servicios. Concluida la vigencia del contrato, los accesos deberán ser eliminados.

e) Procedimientos para la gestión de usuarios privilegiados que incluya la utilización de credenciales de usuarios personalizados, autenticación multifactor, registro de la trazabilidad de las acciones ejecutadas y su monitoreo permanente. Las credenciales de usuarios que vienen configuradas por default en las infraestructuras y plataformas tecnológicas deben ser custodiadas por la unidad de seguridad de la información, y su uso se realizará únicamente en casos excepcionales debidamente justificados y autorizados.

f) Procedimientos para el monitoreo permanente de accesos, operaciones privilegiadas e intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados tanto a nivel interno como con los proveedores que por sus actividades tengan accesos permitidos.

g) Procedimientos que permitan contar con pistas de auditoría a nivel de dispositivos de infraestructura, aplicativos, bases de datos, sistemas operativos, entre otros, que registren los cambios realizados a la información crítica de la entidad. Los administradores no deben tener permiso para borrar ni desactivar las pistas de sus propias actividades.

h) Procedimientos para el uso, protección y tiempo de vida de las llaves criptográficas utilizadas para cifrar la información.

i) Técnicas de cifrado sobre la información que lo requiera como resultado del análisis de riesgos de seguridad.

j) Políticas y controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia; y, para instalar y actualizar periódicamente aplicaciones informáticas para detección y desinfección de virus informáticos y demás software malicioso.

k) La ejecución de auditorías de seguridad de la información que incluya ciberseguridad, con base en el perfil de riesgo de la entidad, por lo menos una (1) vez al año, o antes si se produjeren eventos que ameriten, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar la confidencialidad, integridad y disponibilidad de la información de los servicios que se brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la entidad, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel

internacional; estas auditorías deben incluir, al menos, pruebas de vulnerabilidad y penetración aplicadas a los equipos, dispositivos, canales de comunicación, aplicaciones informáticas, entre otros. Las entidades deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas.

l) La segmentación de la red de datos e implementación de sistemas de control y autenticación tales como: sistemas de prevención de intrusos (IPS), firewalls, firewall de aplicaciones web (WAF), entre otros, con base en un análisis de riesgos, de acuerdo con las necesidades del negocio y conforme la arquitectura tecnológica definida en la entidad; con el fin de minimizar accesos no autorizados inclusive de terceros, especialmente, a la información crítica.

m) Procedimientos para la definición de requerimientos, revisión y actualización de seguridad de la información para nuevos sistemas o su mantenimiento.

n) Escaneo automatizado de vulnerabilidades en código fuente para mitigar los riesgos de seguridad de las aplicaciones previo a su liberación, y de aquellas que se encuentran en producción.

o) Procedimientos de afectación directa a las bases de datos que permitan identificar los solicitantes y autorizadores, y el motivo de la modificación a la información, así como, el registro de pistas de auditoría que facilite la trazabilidad del cambio; y,

p) Procedimientos de difusión, comunicación, entrenamiento y concienciación del sistema de gestión de seguridad de la información, a las partes interesadas internas y externas, según corresponda.

ARTÍCULO 26.- Las entidades controladas deben definir una estrategia y un marco de ciberseguridad alineados a las mejores prácticas internacionales, para preservar la integridad, confidencialidad y disponibilidad de los activos de información, que le permita identificar, proteger, detectar, responder y recuperarse de manera resiliente y oportuna ante amenazas, eventos e incidentes de ciberseguridad tanto internos como externos, para lo cual debe considerar, pero sin limitarse a:

1. Identificar.- Disponer y mantener procesos, prácticas, recursos humanos y tecnológicos, para identificar y evaluar la seguridad cibernética en los procesos de negocio, en busca de debilidades o vulnerabilidad que podrían ser explotadas por actores de amenazas internos y/o externos.

2. Proteger.- Diseñar, implementar y mantener medidas y controles ciberseguridad preventivos de múltiples capas para salvaguardar y defender sus activos tecnológicos.

3. Detectar.- Diseñar, implementar y mantener actividades continuas de detección e identificación oportuna de ocurrencia de eventos de ciberseguridad, a través de: registro continuo y centralizado de eventos de ciberseguridad; gestión de forma oportuna los eventos de ciberseguridad para facilitar la detección y alertas tempranas; y, definición de roles y responsabilidades para la gestión de eventos de ciberseguridad, entre otros.

4. Responder.- Desarrollar e implementar actividades para tomar las medidas oportunas ante un incidente de ciberseguridad detectado y contener su impacto dentro de la Entidad.

Además, la entidad controlada debe asegurar la alineación e integración entre: protocolos de ciberseguridad, infraestructura tecnológica, gestión de crisis, planes de comunicación, y planes de continuidad de negocio para disminuir riesgos que afecten en la continuidad de sus procesos críticos.

5. Recuperar.- Desarrollar e implementar actividades para mantener los planes de resiliencia, para restaurar cualquier capacidad o servicio que se haya visto afectado debido a un incidente de ciberseguridad y la recuperación oportuna a la operación normal.

SECCIÓN IX.- SEGURIDAD EN CANALES ELECTRÓNICOS

ARTÍCULO 27.- Con el objeto de que las transacciones realizadas a través de canales electrónicos cuenten con los controles y mecanismos para evitar el cometimiento de eventos fraudulentos o no autorizados por los usuarios y preservar la seguridad de la información, así como los recursos de los clientes a cargo de las entidades controladas; estas deben cumplir, como mínimo, con lo siguiente:

1. Las entidades controladas deben adoptar e implementar los estándares y buenas prácticas internacionales de seguridad de la información y ciberseguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento.

2. Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como, en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos y para la gestión de tarjetas, de tal manera que, se garantice permanentemente la seguridad; se debe generar informes trimestrales dirigidos al comité de seguridad de la información.

3. Canales de comunicación seguros mediante la utilización de técnicas de cifrado acorde con los estándares internacionales vigentes.

4. Realizar como mínimo una vez al año, o cuando la situación lo amerite, una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por canales electrónicos y para la gestión de tarjetas; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad, se deberá efectuar una prueba adicional.

Las pruebas de vulnerabilidad y penetración deben ser efectuadas por personas natural o jurídica independientes a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las entidades deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas.

Los informes de las pruebas de vulnerabilidad deben estar a disposición de la Superintendencia de Bancos, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior.

5. Transferencia de información de sus clientes relacionada con, al menos, números de cuentas y de tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante mensajería móvil, correo electrónico u otro mecanismo, esta deberá ser enmascarada.

6. La información confidencial debe transmitirse por canales de comunicación seguros debe estar en todo momento protegida mediante el uso de técnicas de cifrado, acorde con los estándares internacionales vigentes y debe evaluarse con regularidad la efectividad del mecanismo utilizado.

7. Las entidades controladas deben contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la entidad.

8. Las entidades controladas deben utilizar tecnología de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos, cuya información en todo momento debe estar cifrada.

9. Establecer procedimientos para monitorear, controlar y emitir alarmas en línea, que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas.

10. Ofrecer a los clientes y/o usuarios los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones monetarias a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad y se debe validar o verificar la autenticidad del cliente a través de métodos de autenticación fuerte.

Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberá constar: el registro de las cuentas favoritas a las cuales desea realizar transacciones monetarias, números de suministros de servicios básicos, números de telefonía fija y móvil; y, montos máximos por transacción por cuenta.

11. Requerir mecanismos de autenticación fuerte para el registro y modificación de la información referente a su número de mensajería móvil y correo electrónico, cuando los clientes los realicen por cualquier canal no presencial o presencial, en cuyo caso, deberá enviarse una notificación a los datos de contacto anteriores y nuevos. La entidad deberá mantener las evidencias respectivas de dichos cambios.

12. Ofrecer a los clientes mecanismos para habilitar o deshabilitar redes de consumo con tarjetas, tales como transacciones: presenciales nacionales, presenciales internacionales; ATM nacional, ATM internacional; internet nacional, internet internacional, entre otros mecanismos que la entidad considere apropiados.

13. Incorporar en los procedimientos de administración de seguridad de la información la renovación de, por lo menos, una vez al año de las claves de acceso a los canales electrónicos y claves de tarjetas; las claves de banca electrónica y banca móvil deben ser diferentes de aquella por la cual se accede a otros canales electrónicos.

14. Las entidades deben establecer procedimientos de control y mecanismos que permitan monitorear las transacciones y el comportamiento de los clientes en el uso de canales electrónicos y tarjetas; para el efecto las entidades deben mantener sistemas digitales e inteligentes de prevención de fraude los mismos que deben alertar al cliente sobre posibles fraudes ante el cambio o uso de su información de datos personales debiendo para tal efecto realizar la debida autenticación fuerte. En tales circunstancias las entidades deben dejar evidencia de lo actuado a través de notificaciones por mensajería móvil y correo electrónico u otro mecanismo conforme a la definición del cliente. Particular que será considerado en el análisis de los reclamos de los usuarios financieros.

15. Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos y/o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas o después de un número máximo de tres intentos de acceso fallido. Además, se deben establecer procedimientos que permitan la notificación en línea al cliente a través mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura.

16. Las entidades controladas deben mantener sincronizados todos los relojes de sus sistemas de información incluidos aquellos que gestionan tarjetas y los dispositivos que estén involucrados con el uso de canales electrónicos.

17. Mantener como mínimo durante doce (12) meses el registro histórico de todas las transacciones que se realicen a través de los canales electrónicos, incluye transacciones realizadas con tarjetas, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta origen y destino en caso de aplicarse, código de la entidad controlada de origen y destino, número de transacción, número de teléfono y correo electrónico al que se notificaron las transacciones y claves de una sola vez; además, para operaciones por cajero automático: código del ATM; para transacciones por internet: la dirección IP; para transacciones a través de sistemas de audio respuesta - IVR: el número de teléfono con el que se hizo la conexión. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales. Si dicha información constituye respaldo contable se aplicará lo previsto en el Código Orgánico Financiero, sobre el archivo de la información.

18. Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción, mediante los aplicativos y bases de datos. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta debe ser enmascarada o codificada por personal independiente al área de desarrollo. Todos estos procedimientos deben estar debidamente documentados en los manuales respectivos.

Además, la entidad debe mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta información debe conservarse por lo menos por doce (12) meses.

19. Las entidades controladas deben poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (call center) u otro medio, para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana; a través de este centro de atención se podrá suspender, bloquear o cancelar el uso de los servicios de canales electrónicos y/o tarjetas con el respectivo procedimiento de seguridad y autenticación del cliente.

20. Mantener, por lo menos, durante doce meses la grabación de las llamadas telefónicas realizadas por los clientes a los centros de atención telefónica (call center), específicamente cuando se consulten saldos, consumos o cupos disponibles; se realicen reclamos; o, se reporten emergencias bancarias; para lo cual, se deben establecer procedimientos que permitan validar de manera segura la identidad del cliente. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales.

21. Las entidades controladas deben enviar a sus clientes mensajes en línea, a través de mensajería móvil y correo electrónico u otro mecanismo, de manera simultánea, notificando la ejecución de transacciones monetarias tales como: pagos, transferencias, retiros y consumos. Para las demás transacciones monetarias la notificación se realizará a través de mensajería móvil o correo electrónico u otro mecanismo conforme a la definición que realice el cliente mediante cualquiera de los canales electrónicos disponibles y/o mediante cualquier medio de pago.

22. Las tarjetas emitidas por las entidades controladas deben contar con microprocesador o chip; además, podrán contar con tecnología NFC (Near Field Communication), y, deben adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo.

23. Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de estos, incluyendo los montos máximos permitidos y los mecanismos para actualizar estos parámetros.

24. Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los canales electrónicos y/o tarjetas ofrecidas por la entidad.

25. En todo momento en donde se solicite el ingreso de una clave, ésta debe aparecer enmascarada.

26. Los pedidos de informes de auditoría interna, realizados por el organismo de control deberán ser atendidos conforme los plazos requeridos.

27. Para el caso de servicios provistos por terceros, asegurar el cumplimiento de las disposiciones incluidas en los numerales precedentes.

28.Las entidades controladas deben ofrecer a sus clientes la matriculación y/o registro de cuentas mediante un método de autenticación fuerte que contemplen una clave de una sola vez OTP (one time password).

ARTÍCULO 28.- Cajeros Automáticos.- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los cajeros automáticos, las entidades controladas deben cumplir con las disposiciones de la "Norma de control para la apertura y cierre de oficinas y canales de las entidades bajo el control de la Superintendencia de Bancos" y, como mínimo, con lo siguiente:

1. Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario deben cifrar la información ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento.

2. La entidad controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado por la entidad controlada a la que pertenece.

3. Los cajeros automáticos deben estar instalados con los estándares de seguridad definidos en las políticas de la entidad controlada, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad.

4. Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos, por lo menos, una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deben ser ejecutados por personal independiente, capacitado y con experiencia; y,

ARTÍCULO 29.- Puntos de venta (POS y PIN Pad).- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los dispositivos de puntos de venta, las entidades controladas deben sujetarse a las medidas de seguridad dispuestas en canales electrónicos y banca electrónica de esta norma, en lo que aplique; y, cumplir, como mínimo, con lo siguiente:

1. Establecer procedimientos que exijan que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta (POS y PIN Pad) en los establecimientos comerciales confirmen su identidad a fin de asegurar que este personal cuenta con la debida autorización.

2. A fin de permitir que los establecimientos comerciales procesen en presencia del cliente o usuario las transacciones monetarias efectuadas a través de los dispositivos de puntos de venta (POS o PIN Pad), éstos deben permitir establecer sus comunicaciones de forma inalámbrica segura.

3.Establecer procedimientos que permitan restringir consumos consecutivos en el mismo establecimiento con tarjetas de crédito y débito.

ARTÍCULO 30.- Banca Electrónica.- Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las entidades controladas que ofrezcan servicios por medio de este canal electrónico deben cumplir, como mínimo, con lo siguiente:

1. Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de cifrado de los datos transmitidos acordes con los estándares internacionales vigentes.

2. Implementar mecanismos de control, y monitoreo que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las entidades controladas.

3. Enviar a sus clientes mensajes en línea a través de mensajería móvil, correo electrónico u otro mecanismo, notificando el acceso a la banca electrónica.

4. Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al cliente para realizar otras transacciones.

5. Informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica. Además, la entidad debe asegurarse de mantener una sola sesión activa independientemente del dispositivo que use el cliente.

6. Implementar mecanismos para detectar la copia de los diferentes componentes de su sitio web, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio (DNS).

7. Implementar mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad.

El nombre de usuario y clave de acceso deben combinar caracteres alfanuméricos con una longitud mínima de seis (6) caracteres; y,

8. Para el ingreso a la banca electrónica, ejecución de transacciones monetarias a cuentas no registradas, así como de operaciones de créditos, se deben implementar métodos de autenticación fuerte que contemplen, por lo menos, dos (2) de tres (3) factores: “algo que se sabe, algo que se tiene o algo que se es”, considerando que uno de ellos debe: ser dinámico por cada vez que se efectúa una transacción, ser una clave de una sola vez OTP (one time password), tener controles biométricos, token virtual, entre otros.

ARTÍCULO 31.- Banca Móvil.- Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca móvil desde dispositivos y números telefónicos autorizados, las entidades controladas que ofrezcan servicios por medio de este canal electrónico deben cumplir con los numerales 3,4,5,7,8 del artículo 30 de Banca Electrónica.

ARTÍCULO 32.- Las entidades controladas que presten servicios a través de IVR deben sujetarse, en lo que corresponda, a las medidas de seguridad dispuestas en canales electrónicos y banca electrónica de esta norma.

ARTÍCULO 33.- Las entidades controladas que presten servicios a través de corresponsales no bancarios deben sujetarse, en lo que corresponda, a las medidas de seguridad de la información y ciberseguridad, canales electrónicos, banca electrónica, POS y PIN Pad dispuesta en esta norma.

DISPOSICIONES GENERALES

PRIMERA.- Las entidades controladas contratarán anualmente con las compañías de seguro privado pólizas de los ramos autorizados por el organismo de control pertinente, que incluyan coberturas que aseguren a las entidades contra fraudes generados a través de: sistemas de cómputo, programas electrónicos de computadoras, datos y medios electrónicos, virus de computadoras, comunicaciones electrónicas o telefax, transmisiones electrónicas, valores electrónicos y similares, como mínimo, ante los siguientes riesgos:

a) Revelación ilegal de bases de datos;
b) Interceptación ilegal de datos;
c) Transferencia electrónica del activo patrimonial; y,
d) Ataque a la integridad a los sistemas informáticos.

SEGUNDA.- La Superintendencia de Bancos, como resultado de las evaluaciones que realice, podrá disponer la adopción de medidas adicionales a las previstas en la presente norma, con el propósito de reducir la exposición al riesgo operativo que enfrenten las entidades controladas.

TERCERA.- Las entidades controladas deberán reportar trimestralmente el Valor de Riesgo Operativo definido como la multiplicación entre los ingresos brutos por segmento por un coeficiente marginal de acuerdo al segmento.

$$\boldsymbol{VRO} = \sum(\boldsymbol{\alpha_i} * \boldsymbol{Yb_i});$$

Donde;

Ybi = es el ingreso bruto (i, denota los segmentos), y;

αi =es un coeficiente marginal diferenciado por tipo de entidad.

Para el efecto el ente de control emitirá una nota metodológica con la descripción detallada del cálculo.

CUARTA.- El ente de control emitirá una nota metodológica para el reporte mediante estructura de datos los riesgos y eventos de riesgos operativos que las entidades deberán reportar trimestralmente.

QUINTA.- El ente de control en cualquier momento puede realizar una supervisión a fin de verificar la implementación de la presente norma.

SEXTA.- La Superintendencia de Bancos definirá la información que se requiera para la implementación de la presente norma.

SÉPTIMA.- Los casos de duda y los no contemplados en la presente norma, serán resueltos por la Superintendencia de Bancos.

DISPOSICIONES TRANSITORIAS

PRIMERA.- Las disposiciones contenidas en la presente norma relacionados con Seguridad de la Información, Canales Electrónicos, Continuidad del Negocio y Servicios provistos por Terceros serán implementadas por las entidades controladas en el plazo de 120 días, los demás deben ser implementados en el plazo de 150 días a partir de su expedición, la verificación del cumplimiento de las disposiciones debe ser revisado y validado por la unidad de Auditoría Interna

y remitido en sus informes periódicos. (reformada por Resolución No. SB-2023-02343 de 13 de noviembre de 2023).

SEGUNDA.- Las disposiciones contenidas en la sección de Gestión de Incidentes y Problemas deben ser implementadas hasta máximo el 31 de diciembre de 2023. (reformada por Resolución No. SB-2023-02343 de 13 de noviembre de 2023).

ANEXO 1. EVENTOS DE RIESGO OPERATIVO DE ACUERDO CON BASILEA

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Ejemplos de actividades (Nivel 3)
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa	Actividades no autorizadas	i) Operaciones no reveladas intencionalmente; ii) Operaciones no autorizadas con pérdidas monetarias; y iii) Valoración errónea intencional de posiciones
		Hurto y fraude	i) Fraude / fraude crediticio/ depósitos sin valor Hurto / extorsión / malversación / robo; ii) Apropiación indebida de activos; iii) Destrucción dolosa de activos; iv) Falsificación; v) Utilización de cheques sin fondos; vi) Contrabando; vii) Apropiación de cuentas, de identidad, etc.; viii) Incumplimiento / evasión intencional de impuestos; ix) Soborno / cohecho; y x) Abuso de información privilegiada
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero	Hurto y fraude	i) Hurto/ robo; ii) Falsificación; y iii) Utilización de cheques sin fondos
		Seguridad de los sistemas	i) Daños por ataques informáticos; y ii) Robo de información con pérdidas monetarias
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la discriminación	Relaciones laborales	i) Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos; y ii) Organización laboral
		Higiene y seguridad en el trabajo	i) Imposibilidad en general (resbalones, caídas, etc.); ii) Casos relacionados con las normas de higiene y seguridad en el trabajo; y iii) Indemnización a los trabajadores
		Diversidad y discriminación	Todo tipo de discriminación
Incidencias en el negocio y fallos en los sistemas	Pérdidas derivadas de interrupción en los negocios o por fallas en los sistemas	Sistemas	i) Hardware; ii) Software; iii) Telecomunicaciones; y iv) Interrupción / incidencias en el suministro

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Ejemplos de actividades (Nivel 3)
Daños a activos materiales	Pérdidas derivadas por daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros eventos	Desastres y otros acontecimientos	i) Pérdidas por desastres naturales; ii) Pérdidas humanas por causas externas (terrorismo, vandalismo)
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto	Adecuación, divulgación de información y confianza	i) Abusos de confianza / incumplimiento de pautas; ii) Apropiamiento / divulgación de información; ii) Violación de la privacidad de clientes minoristas; iii) Quebrantamiento de privacidad; iv) Ventas agresivas; v) Pérdidas de cuentas; vi) Mal uso de información confidencial; y vii) Responsabilidad del prestamista
		Prácticas empresariales o de mercado impropias	i) Prácticas anti-competencia; ii) Prácticas impropias comerciales y de mercado; iii) Manipulación del mercado; iv) Comercialización de información privilegiada a favor de la empresa; v) Actividades no autorizadas; y vi) Lavado de dinero
		Productos defectuosos	i) Defectos del producto; y ii) Error de modelo
		Selección, patrocinio y riesgos	i) Fallida investigación a clientes según los protocolos; y ii) Superación de los límites de exposición frente a clientes
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	i) Comunicación defectuosa; ii) Errores de introducción de datos, mantenimiento o descarga; iii) Incumplimiento de plazos o de responsabilidades; iv) Ejecución errónea de modelos / sistemas; v) Error contable / atribución a entidades erróneas; vi) Errores en otras tareas; vii) Fallo en la entrega; viii) Fallo en la gestión del colateral; y ix) Mantenimiento de datos de referencia

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Ejemplos de actividades (Nivel 3)
		Seguimiento y monitoreo	i) Incumplimiento en la obligación reportar; y ii) Inexactitud de informes externos (incurriendo en pérdidas)
		Aceptación de clientes y documentación	i) Extravío de autorizaciones / rechazos de clientes; y ii) Documentos jurídicos inexistentes / incompletos
		Gestión de cuentas de clientes	i) Acceso no autorizado a cuentas; ii) Registros incorrectos de clientes (incurriendo en pérdidas); y iii) Pérdida o daño de activos de clientes por negligencia
		Contrapartes comerciales	i) Fallos con contrapartes no-clientes; y ii) Otros litigios con contrapartes distintas de clientes
		Distribuidores y proveedores	i) Subcontratación; y ii) Litigios con distribuidores