# EL COMITÉ DE NORMAS DEL BANCO CENTRAL DE RESERVA DE EL SALVADOR,

**CONSIDERANDO:**

1. Que de conformidad al artículo 2, inciso segundo de la Ley de Supervisión y Regulación del Sistema Financiero, para el buen funcionamiento del Sistema de Supervisión y Regulación Financiera se requiere que los integrantes del sistema financiero y demás supervisados cumplan con las regulaciones vigentes y la adopción de los más altos estándares de conducta en el desarrollo de sus negocios, actos y operaciones, de conformidad a lo establecido en la referida Ley, en las demás leyes aplicables, en los reglamentos y en las normas técnicas que se dicten para tal efecto.
2. Que de conformidad al artículo 35, inciso primero y literal d) de la Ley de Supervisión y Regulación del Sistema Financiero, los directores, gerentes y demás funcionarios que ostenten cargos de dirección o de administración en los integrantes del sistema financiero, deben conducir sus negocios, actos y operaciones cumpliendo con los más altos estándares éticos de conducta y actuando con la diligencia debida de un buen comerciante en negocio propio, estando obligados a cumplir y a velar por que en la institución que dirigen o laboran se cumpla con la adopción y actualización de políticas y mecanismos para la gestión de riesgos, debiendo entre otras acciones, identificarlos, evaluarlos, mitigarlos y revelarlos acordes a las mejores prácticas internacionales.
3. Que el artículo 7 de la Ley de Supervisión y Regulación del Sistema Financiero, establece las entidades que están sujetas a la supervisión de la Superintendencia del Sistema Financiero.
4. Que de conformidad al artículo 99, literales a) y g) de la Ley de Supervisión y Regulación del Sistema Financiero, el Banco Central de Reserva de El Salvador es la institución responsable de la aprobación de normas técnicas relativas a la gestión de riesgos por parte de los supervisados, así como aquellas en las que se definan las condiciones mínimas que deben reunir físicamente los locales, sus medidas de seguridad, lo relativo a la conservación y archivo de documentación de los integrantes del sistema financiero.
5. Que los estándares internacionales sugieren, entre otras actividades de buenas prácticas, guías amplias en materia de continuidad de negocio, con la descripción de los métodos, técnicas y enfoques utilizados en todo el mundo para desarrollar, implementar y mantener un sistema eficaz de gestión de continuidad del negocio.
6. Que es conveniente que las entidades gestionen adecuadamente los riesgos a los que están expuestos los diferentes procesos y actividades, de manera que garanticen la continuidad del negocio, velando por una gestión eficiente del riesgo operacional.

**POR TANTO,**

en virtud de las facultades normativas que le confiere el artículo 99 de la Ley de Supervisión y Regulación del Sistema Financiero,

**ACUERDA,** emitir las siguientes:

**NORMAS TÉCNICAS PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**

**CAPÍTULO I**

**OBJETO, SUJETOS Y TÉRMINOS**

**Objeto**

1. Las presentes Normas tienen como objeto establecer las disposiciones mínimas que deben considerar las entidades para la Gestión de la Continuidad del Negocio y criterios para la adopción de políticas y procedimientos relacionados con el desarrollo de metodologías para su respectiva gestión, acordes a las mejores prácticas internacionales, el tamaño, naturaleza de sus operaciones, segmentación de negocios y la complejidad organizacional de cada entidad y, de esta forma, fortalecer su gestión de riesgos operacionales.

**Sujetos**

1. Son sujetos de las presentes Normas las entidades siguientes:
2. Los bancos constituidos en El Salvador, sus oficinas en el extranjero y sus subsidiarias; las sucursales y oficinas de bancos extranjeros establecidos en el país;
3. Las sociedades que de conformidad con la ley, integran los conglomerados financieros, o que la Superintendencia del Sistema Financiero declare como tales, lo que incluye tanto a sus sociedades controladoras como a sus sociedades miembros;
4. Las instituciones administradoras de fondos de pensiones;
5. Las sociedades de seguros, sus sucursales en el extranjero y las sucursales de sociedades de seguros extranjeras establecidas en el país;
6. Las bolsas de valores, las casas de corredores de bolsa, las sociedades especializadas en el depósito y custodia de valores, las clasificadoras de riesgo, los agentes especializados en valuación de valores y los almacenes generales de depósito;
7. Los bancos cooperativos, las sociedades de ahorro y crédito y las federaciones reguladas por la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito;
8. Las sociedades de garantía recíproca y sus reafianzadoras locales;
9. Las sociedades que ofrecen servicios complementarios a los servicios financieros de los integrantes del sistema financiero, en particular aquellas en los que participen como inversionistas;
10. Las sociedades administradoras u operadoras de sistemas de pagos y de liquidación de valores;
11. El Fondo Social para la Vivienda y el Fondo Nacional de Vivienda Popular;
12. El Instituto Nacional de Pensiones de los Empleados Públicos y el Instituto Salvadoreño del Seguro Social, este último en lo relativo al Sistema de Pensiones Público, al Régimen de Riesgos Profesionales y reservas técnicas de salud;
13. El Instituto de Previsión Social de la Fuerza Armada;
14. El Banco de Fomento Agropecuario, el Banco Hipotecario de El Salvador, S.A. y el Banco de Desarrollo de El Salvador;
15. Las titularizadoras y los fondos que administran;
16. Las bolsas de productos y servicios;
17. Las Gestoras de fondos de inversión y los fondos que administran;
18. Las Empresas de Transferencia de Dinero y los Agentes cuyo país de origen sea El Salvador de acuerdo a lo establecido en las “Normas Técnicas para el Registro, Obligaciones y Funcionamiento de Entidades que Realizan Operaciones de Envío o Recepción de Dinero” (NRP-12); y
19. Las Sociedades Proveedoras de Dinero Electrónico.

**Términos**

1. Para efectos de las presentes Normas, los términos que se indican a continuación tienen el significado siguiente:
2. **Alta Gerencia:** El Presidente Ejecutivo, Gerente General o quien haga sus veces y los cargos ejecutivos que le reporten al mismo;
3. **Amenaza:** La potencial ocurrencia de un evento no deseado, puede entenderse como un peligro que está latente, y que pueda afectar la continuidad del negocio;
4. **Análisis de Impacto del Negocio (**BIA, por sus siglas en inglés**):** Proceso por el que se analizan las funciones y actividades del negocio y las consecuencias que generaría sobre ellas, la ocurrencia de eventos no deseados;
5. **Banco Central:** Banco Central de Reserva de El Salvador;
6. **Ciberamenaza o amenaza cibernética:** Potencial ocurrencia de una situación que pudiera convertirse en un ciberataque;
7. **Ciberataque o ataque cibernético:** acción organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio, o donde el ciberespacio es fuente o herramienta, para la materialización de un perjuicio que compromete la seguridad de la información de la entidad;
8. **Ciberespacio:** entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física;
9. **Ciberseguridad:** es el desarrollo de capacidades técnicas para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar la información, infraestructura o plataforma tecnológica y aplicaciones en el ciberespacio y que son esenciales para la operación de la entidad;
10. **Continuidad del Negocio:** es la capacidad de una entidad para seguir ofreciendo sus productos o servicios a niveles previamente definidos como aceptables después de un incidente de interrupción;
11. **Cultura Organizacional:** es el conjunto de actitudes, creencias, comportamientos, normas y valores aceptados y aplicados cotidianamente por los miembros de una entidad en la interacción entre sus miembros y en su interacción con el exterior;
12. **Entidad:** sujeto obligado al cumplimiento de las disposiciones de las presentes Normas, descrito en el artículo 2 de las mismas;
13. **Evento:** un suceso o serie de sucesos que pueden ser internos o externos a la entidad, originados por la misma causa, que ocurren durante el mismo período de tiempo;
14. **Evento no deseado:** evento que interrumpe, daña o altera los procesos o recursos de la entidad que están relacionados a los productos y servicios que esta ofrece;
15. **Gestión de la Continuidad del Negocio: p**roceso de gestión integral que identifica amenazas, ciberamenazas y ciberataques potenciales a una entidad y el impacto que podrían causar a las operaciones del negocio, en caso de materializarse. Este proceso provee un marco para construir la capacidad organizacional de sobreponerse a un evento disruptivo y ofrecer una respuesta efectiva, de tal manera de salvaguardar los objetivos corporativos, reputación, marca y actividades de creación de valor;
16. **Gestión de crisis:** proceso mediante el cual una entidad afronta uno o varios eventos de considerable magnitud que amenazan con afectar financiera, económica y reputacionalmente a la entidad y partes interesadas, frente a sus clientes, usuarios o al público en general. Dichos eventos podrían no implicar la disrupción de las operaciones de la entidad, tales como la difusión o publicación de información que podría dañar la reputación de la misma;
17. **Incidente de interrupción:** un evento que tiene la capacidad de generar una interrupción en los productos o servicios que ofrece una entidad, el cual, de no ser gestionado apropiadamente, puede ocasionar una emergencia, crisis o desastre. Se le conoce también como incidente disruptivo;
18. **Junta Directiva:** órgano colegiado encargado de la administración de la entidad, con funciones de supervisión y control. Para el caso de las Asociaciones Cooperativas será el Consejo de Administración;
19. **Máximo Período Tolerable de Disrupción (**MTPD, por sus siglas en inglés**):** es el período después del cual la entidad es afectada de manera irreparable porque la entrega de productos y servicios no puede ser reanudada;
20. **Objetivo Mínimo de Continuidad de Negocio (**MBCO, por sus siglas en inglés**):** es el mínimo nivel aceptable de productos o servicios que una entidad debe ofrecer para alcanzar sus objetivos durante un incidente de interrupción;
21. **Partes interesadas:** personas u organizaciones que se ven impactadas por las operaciones de una entidad. Ejemplos: empleados, clientes, socios del negocio, proveedores, accionistas, instituciones gubernamentales, entre otros;
22. **Plan de Continuidad del Negocio** (BCP, por su siglas en inglés)**:** procedimientos documentados que guían a las entidades para responder, recuperar y continuar con el negocio a un nivel de operación predefinido como aceptable, posterior a un incidente de interrupción;
23. **Proceso:** se refiere al conjunto de procedimientos, actividades y tareas organizadas, interrelacionadas y repetibles que producen un resultado esperado;
24. **Procesos de contingencia:** procedimientos documentados que guían a las entidades sobre cómo actuar ante eventos concretos o incidentes de interrupción. Se centran en la atención de riesgos operativos y fallas frecuentes;
25. **Prueba(s):** simulación de una interrupción de los procesos u operaciones para evaluar los componentes de un plan (por ejemplo, tareas, equipos, personal, procedimientos, entre otros) con el objetivo de comprobar si es viable y funcional;
26. **Producto y servicio:** resultados beneficiosos proporcionados por la entidad a sus potenciales clientes, destinatarios y partes interesadas;
27. **Punto Objetivo de Recuperación** (ROP, por sus siglas en inglés)**:** representa la máxima pérdida de datos admisible para que continúe siendo factible reanudar una operación y es expresado en unidades de tiempo de información perdida;
28. **Riesgo:** la condición en que existe la posibilidad de que un evento ocurra e impacte negativamente los objetivos de la empresa;
29. **Riesgo operacional:** posibilidad de incurrir en pérdidas debido a fallas en los procesos, de las personas, en los sistemas de información y a causa de acontecimientos externos, incluye el riesgo legal;
30. **Sistema de Gestión de la Continuidad del Negocio (SGCN):** es parte del sistema general de gestión que establece, implementa, opera, monitorea, revisa, mantiene y mejora la continuidad del negocio. Es decir, brinda un método formal para poner en marcha la Gestión de la Continuidad del Negocio y verificar que es efectivo y consistente con los niveles de continuidad definidos y la cultura organizacional;
31. **Superintendencia:** Superintendencia del Sistema Financiero;
32. **Tercerización de servicios:** se produce cuando la entidad encarga la realización de un proceso a un tercero, es decir, a una persona natural o jurídica distinta a la entidad; y
33. **Tiempo Objetivo de Recuperación** (RTO, por sus siglas en inglés)**:** es el tiempo establecido por la entidad para reanudar la entrega de un producto o servicio luego de un incidente de interrupción. El RTO de cada producto, servicio, proceso o actividad es menor que el respectivo Máximo Periodo Tolerable de Disrupción.

**CAPÍTULO II**

**ROLES Y RESPONSABILIDADES GENERALES**

**Gestión de la continuidad del negocio**

1. La Junta Directiva, la Alta Gerencia y el personal deben gestionar permanentemente la continuidad del negocio de las entidades. La gestión de la continuidad del negocio de las entidades debe ser adecuada a la naturaleza, tamaño y complejidad de las operaciones, productos y servicios que ofrecen.

En tal sentido, las entidades deben contar con una estructura organizacional o funcional que delimite claramente las funciones, roles y responsabilidades específicas asociadas a la continuidad del negocio, así como los niveles de dependencia e interrelación que corresponde con cada una de las demás áreas de la entidad.

Asimismo, cuando el tamaño y complejidad de operaciones y servicios de la entidad lo amerite, la función de continuidad del negocio será desempeñada por una unidad o área especializada y que garantice su reporte a la Junta Directiva**.**

**Responsabilidades de la Junta Directiva**

1. La Junta Directiva será la responsable de establecer una adecuada gestión de la continuidad del negocio, por lo que debe realizar al menos lo siguiente:
2. Aprobar una política de continuidad del negocio, de conformidad a lo establecido en el artículo 11 de las presentes Normas;
3. Aprobar el Sistema de Gestión de Continuidad del Negocio;
4. Fomentar el desarrollo de una cultura de continuidad, motivando la participación activa y el compromiso de todos los empleados;
5. Aprobar los recursos necesarios para el adecuado desarrollo e implementación de la gestión de la continuidad del negocio acordes a los resultados del análisis de impacto de negocio, a fin de contar con la infraestructura, metodología y personal apropiados;
6. Aprobar el plan de continuidad del negocio;
7. Verificar que la entidad cuenta con una efectiva gestión de la continuidad del negocio;
8. Autorizar la validación del plan de continuidad del negocio a la unidad que desempeñe la función de continuidad del negocio, de conformidad a los procedimientos establecidos en los artículos 17, 18, 19 y 20 de las presentes Normas; y
9. Promover la mejora continua en la gestión de continuidad del negocio de la institución.

**Responsabilidades de la Alta Gerencia**

1. En cuanto a la gestión de la continuidad del negocio, la Alta Gerencia tendrá al menos la responsabilidad de las actividades siguientes:
2. Implementar y apoyar la gestión de la continuidad del negocio conforme a las disposiciones de la Junta Directiva; y
3. Promover la mejora continua del Sistema de Gestión de la Continuidad del Negocio y velar por su vigencia permanente.

**Responsabilidades del Comité de Riesgos**

1. En materia de gestión de la continuidad del negocio, el Comité de Riesgos será el responsable al menos de lo siguiente:
2. Revisar, evaluar y proponer a la Junta Directiva la política de continuidad del negocio para su aprobación;
3. Proponer, para aprobación de la Junta Directiva, la estructura del Sistema de Gestión de la Continuidad del Negocio;
4. Revisar, evaluar y proponer a la Junta Directiva los planes de continuidad del negocio para su aprobación;
5. Apoyar la labor de quien posea la función de continuidad de negocio en la implementación de la gestión de continuidad del negocio;
6. Efectuar el seguimiento de la gestión de continuidad del negocio.
7. Recomendar la implementación de mecanismos adicionales en la ejecución de pruebas, de tal forma que una vez finalizadas resulten satisfactorias; y
8. Validar el resultado satisfactorio de las pruebas realizadas.

Cuando el número de las operaciones o la estructura organizativa de la entidad no permita la creación del Comité de Riesgos, las funciones correspondientes podrán ser desarrolladas por la Junta Directiva de la entidad o por un Comité de Riesgos Corporativo, siempre que cumpla con lo dispuesto en el marco legal aplicable y con las disposiciones establecidas en las presentes Normas, garantizándose la objetividad, el adecuado manejo de conflictos de interés, independencia de criterio, confidencialidad y acceso a la información. En estos casos, la entidad será responsable de contar con las actas, informes y documentación de respaldo de los temas revisados.

La Junta Directiva de la entidad mantendrá la responsabilidad sobre la ejecución de las funciones definidas en las presentes Normas. En el caso de las sucursales de bancos extranjeros establecidos en el país y sucursales de Sociedades de Seguros Extranjeras establecidas en el país, el Comité de Riesgos estará constituido por su Representante o quien haga sus veces, un funcionario de la Alta Gerencia y un Ejecutivo que tenga como responsabilidad la gestión de los riesgos de la entidad.

El Comité estará presidido por uno de sus miembros que tenga conocimiento en finanzas. El Comité de Riesgos cumplirá como mínimo con las disposiciones establecidas en las Normas relativas a la Gestión de Riesgos que para tales efectos emita el Banco Central por medio de su Comité de Normas.

**Responsabilidad de la Unidad de Riesgos**

1. En materia de gestión de la continuidad del negocio, la Unidad de Riesgos debe llevar a cabo como mínimo lo siguiente:
2. Revisar y evaluar los elementos del Sistema de Gestión de Continuidad del Negocio;
3. Asegurar que la gestión de la continuidad del negocio que realice la entidad sea consistente con las políticas y procedimientos aplicados para la gestión de riesgos y con la dirección estratégica; y
4. Evaluar si existe la necesidad de constituir comités, unidades o áreas especializadas para el cumplimiento de las responsabilidades relacionadas con la gestión de la continuidad del negocio. De ser necesario, presentará su propuesta al Comité de Riesgos, para que este someta a aprobación de la Junta Directiva la creación de dicho Comité o Unidad.

Cuando el número de las operaciones o la estructura organizativa de la entidad no permita la creación de la Unidad de Riesgos, la Junta Directiva deberá designar una persona de la entidad, según aplique, y proveerle los recursos suficientes para desempeñar su función conforme al tamaño, estructura y perfil de riesgo de la entidad; en todo caso, deberá asegurarse que exista independencia de ésta con las áreas de negocio y operativas, a fin de evitar conflictos de interés y asegurar una adecuada separación de funciones y responsabilidades.

Su posición jerárquica deberá asegurar que sus informes sean conocidos por la Junta Directiva o por la instancia que ésta delegue.

**CAPÍTULO III**

**DEL SISTEMA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**

**Sistema de Gestión de la Continuidad del Negocio**

1. Las actividades mínimas que las entidades deben desarrollar para implementar un SGCN serán las siguientes:
2. Establecer una política de continuidad del negocio;
3. Definir roles y responsabilidades de los participantes en la gestión de continuidad del negocio;
4. Realizar el análisis de impacto del negocio y su respectiva evaluación de riesgos;
5. Diseñar y seleccionar las estrategias y tácticas de continuidad del negocio;
6. Desarrollar e implementar la estrategia de continuidad de negocio seleccionada;
7. Elaborar planes de continuidad del negocio para los procesos que permitan la entrega de productos y servicios críticos que la entidad ofrece;
8. Probar y actualizar los planes de continuidad del negocio, de conformidad a lo dispuesto en los artículos 17, 18, 19 y 20 de las presentes Normas;
9. Integrar la gestión de la continuidad del negocio dentro de la cultura organizacional a través de la capacitación, divulgación y concientización del personal, al menos una vez al año;
10. Definir una estrategia de gestión de crisis;
11. Documentar los cambios significativos que arrojaron las pruebas realizadas a los de planes de continuidad así como la actualización de estos con base a dichos cambios; y
12. Efectuar revisiones del SGCN, al menos una vez al año.

#### Funciones de la unidad o área especializada en Continuidad del Negocio

1. La función de continuidad del negocio comprenderá al menos los aspectos siguientes:
2. Velar por la gestión de la continuidad del negocio, asegurándose que se realicen las actividades mínimas del SGCN mencionadas en el artículo 9 de las presentes Normas;
3. Elaborar la política de continuidad del negocio y proponerla al Comité de Riesgos o quien haga sus veces para su revisión y evaluación;
4. Diseñar la estructura del SGCN y proponerla al Comité de Riesgos para su revisión y evaluación;
5. Mantener un registro de los incidentes que afecten la continuidad del negocio, para ello deberán mantener un historial de los mismos y ser oportunamente comunicados a las altas autoridades de la entidad y a la Superintendencia;
6. Coordinar entre las diversas áreas de negocio relevantes de la entidad, la ejecución de cada una de las actividades mínimas del SGCN;
7. Consolidar las estrategias y tácticas, entre otros elementos, de los diversos planes que conforman el plan de continuidad del negocio;
8. Mantener informes sobre los aspectos relevantes de la gestión de la continuidad del negocio para una oportuna toma de decisiones;
9. Elaborar y proponer al Comité de Riesgos o quien haga sus veces, el plan de continuidad del negocio para su revisión y evaluación;
10. Elaborar y ejecutar planes anuales de capacitación del personal para que éste conozca su rol a la hora de enfrentar un evento disruptivo;
11. Definir un responsable de informar a la Superintendencia la activación del plan de continuidad del negocio, los resultados de las pruebas que hayan realizado sobre éste, la documentación que soporte todo lo anterior, así como cuando se inicie una gestión de crisis. Dicha comunicación deberá realizarse a más tardar un día después de ocurrido un evento de disrupción; y para el caso de las entidades que se conectan directamente con el sistema de Liquidación Bruta en Tiempo Real del Banco Central, la información mencionada en este literal también deberá ser remitida a éste último; y
12. Informar al Comité de Riesgos sobre el resultado de las pruebas realizadas.

**Política de la Continuidad del Negocio**

1. La política de la continuidad del negocio debe surgir de la adaptación de la definición de continuidad de negocio para la entidad y compatible con las presentes Normas. Para ello, debe definir el alcance, principios y guías que orientarán la gestión de la continuidad del negocio acordes con la naturaleza, tamaño, perfil de riesgo y volumen de operaciones de la entidad. Dicha política, deberá adecuarse al propósito y a las necesidades de la entidad, estableciendo claramente lo que debe lograr en la gestión de la continuidad del negocio. Asimismo, debe ser concisa, clara y precisa, debiendo ser comunicada a todo el personal de la entidad.

La política de la continuidad del negocio incluirá al menos lo siguiente:

1. Los roles y responsabilidades específicos asociados con la gestión de la continuidad del negocio;
2. Un conjunto de principios, guías y normas mínimas para la continuidad del negocio; y
3. Criterios mínimos para la definición de un presupuesto que permita el desarrollo e implementación de la gestión de la continuidad del negocio. Para dicha definición deberá realizarse una evaluación de los recursos necesarios para la ejecución de los procedimientos de continuidad de la entidad.

**Incorporación de la Continuidad del Negocio en la Cultura Organizacional**

1. La entidad debe incorporar el concepto e importancia de la continuidad de negocio en la cultura organizacional, de tal manera que todo el personal labore con un enfoque de continuidad del negocio; es decir, que reconozca a la continuidad del negocio como un objetivo prioritario y completamente alineado a la gestión estratégica y cotidiana de la entidad.

Para asegurar que la continuidad del negocio está siendo incorporada en la cultura organizacional, la entidad deberá implementar, por lo menos, los aspectos siguientes:

1. La Junta Directiva dará seguimiento a la continuidad del negocio, al menos una vez al año y cada vez que ocurran cambios significativos que impliquen la actualización del plan de continuidad del negocio;
2. Desarrollar sesiones de concientización de la continuidad del negocio en las capacitaciones del personal o procesos de inducción, de conformidad a lo establecido en las presentes Normas; y
3. Los ejercicios o pruebas de continuidad del negocio se desarrollarán según lo programado y con los propios recursos y procesos de contingencia que realmente ocupa la entidad para llevar a cabo sus operaciones o procesos diariamente, debiendo documentarse la realización de dichas pruebas o ejercicios.

**Análisis de Impacto del Negocio**

1. Para efectos de determinar los productos o servicios críticos y como base para la gestión de la continuidad del negocio, la entidad debe contar con un análisis de impacto del negocio o AIN.

El AIN debe tomar en cuenta todos los productos y servicios que una entidad entrega; además debe identificar, cuantificar y calificar las ciberamenazas y los impactos de incidentes de interrupción en términos financieros, reputacionales y de tiempo.

Lo anterior implica que la entidad debe aplicar la política de continuidad del negocio antes del lanzamiento de un nuevo producto o servicio, o ante cambios significativos en su operatividad.

Asimismo, el AIN deberá implicar la definición de plazos prioritarios para la reanudación de las actividades a un nivel aceptable mínimo especificado y señalar las dependencias y recursos de apoyo para estas actividades.

Los AIN deben ser revisados y actualizados anualmente y en la misma oportunidad en que se actualiza el plan estratégico de la entidad, así como cuando existan cambios relevantes en los procesos o infraestructura tecnológica y que puedan afectar significativamente cada actividad, proceso y productos o servicios críticos.

**Análisis de ciberamenazas, amenazas y evaluación de riesgos**

1. La metodología de evaluación de las ciberamenazas y amenazas debe ser coherente con el Análisis de Impacto del Negocio realizado y con la metodología de evaluación de riesgos empleada por la entidad para los riesgos operacionales y puede ser aplicada con mayor frecuencia si existe un cambio significativo, interno o externo, a la entidad.

Los análisis de ciberamenazas y amenazas deben considerar diversas fuentes, entre ellas las de índole geográfico, sociopolítico, pandémico, físico, ambiental y tecnológico. Además debe evaluar el impacto, por lo menos, en los siguientes ámbitos: finanzas, clientes, personal, cumplimiento regulatorio y opinión pública. El impacto total de una actividad, proceso, producto o servicio podrá ser cuantificado ponderando el impacto en cada uno de los ámbitos antes mencionados.

El resultado del análisis de las ciberamenazas y amenazas es una lista de las mismas de procedencia interna o externa que pueden provocar una alteración de las actividades críticas de la entidad, con prioridad por nivel de impacto total. Sobre esta base se elaborarán escenarios de interrupción para los cuales se deberán diseñar estrategias concretas que permitan a la entidad manejar un incidente de interrupción.

**Selección de la estrategia de continuidad**

1. La definición de las estrategias, tácticas de continuidad y recuperación que deben llevar a cabo todo el personal de la entidad, para la reanudación de las actividades críticas, requerirá de la aprobación de la Junta Directiva y deberá tomar en cuenta como mínimo, los aspectos siguientes:
2. La seguridad del personal;
3. Las habilidades y conocimientos asociados a cada proceso crítico;
4. Las instalaciones alternas de trabajo;
5. Una infraestructura alterna de tecnología de información y comunicaciones;
6. El equipamiento necesario; y
7. La seguridad y ciberseguridad de la información.

**Desarrollo e implementación de la estrategia de continuidad**

1. Para el desarrollo e implementación de la estrategia de continuidad, las entidades ejecutarán dichas estrategias y tácticas definidas, realizando al menos las actividades siguientes:
2. Definir planes de continuidad a nivel estratégico, táctico y operativo en los que se documenten las prioridades, procedimientos, responsabilidades, recursos implicados, entre otros, que permitan a la entidad manejar un incidente de interrupción de productos y servicios críticos;
3. Definir un procedimiento claro y conocido por todo el personal involucrado en la activación y desactivación de los planes, así como para el control de los procedimientos de respuesta de la entidad a los incidentes de interrupción de los productos y servicios críticos;
4. Actualizar constantemente al personal involucrado en la gestión de la continuidad del negocio, conforme a los roles y responsabilidades derivados de la política de continuidad del negocio, para la aplicación de las estrategias y tácticas de continuidad establecidas y el desarrollo de sus operaciones cotidianas con los procedimientos alternativos que pudiese tener la entidad, cuando sea el caso;
5. Definir mecanismos que aseguren la capacidad de comunicarse de manera efectiva con las partes interesadas internas y externas a la entidad;
6. Destinar los recursos suficientes para la implementación de las estrategias de continuidad aprobadas por la Junta Directiva durante la selección de la estrategia de continuidad;
7. Evaluar, en el caso de entidades que pertenecen a conglomerados financieros, la necesidad de obtener el consenso de las empresas del grupo sobre la priorización de las actividades de recuperación, uso de instalaciones y recursos compartidos, entre otros, para la implementación de estrategias y tácticas de continuidad conjuntas; y
8. Tener todo dispuesto para que los planes puedan ser activados en cualquier instante y sean ejecutados con eficiencia y efectividad.

**Validación del Plan de Continuidad del Negocio**

1. Las entidades deben confirmar, mediante las actividades a que hace referencia el artículo 19 de las presentes Normas, que la gestión de la continuidad del negocio cumple con los objetivos fijados en la política de continuidad del negocio y que el plan de continuidad es idóneo para la entidad y las amenazas identificadas. La entidad no podrá argumentar la existencia de un plan de continuidad si éste no ha sido validado.
2. La validación del plan de continuidad del negocio de la entidad implica que debe ejecutar como mínimo, pruebas anuales o cuando surja un cambio significativo en el referido plan.

Los tipos de pruebas que deben desarrollarse, al menos, son las siguientes:

1. De Escritorio: Método de ensayo para ejercitar los planes, en el que los participantes revisan y discuten los planes de acción y procedimientos sin ejecutarlos, en un ambiente seguro y libre de estrés. Puede llevarse a cabo con uno o varios equipos o departamentos. Por lo general, requiere la guía de un facilitador;
2. Simulaciones: su proceso implica utilizar una situación creada para validar la información del plan, generando una respuesta teórica del incidente;
3. De Funciones: ejecución de los planes y procedimientos de recuperación de un área o línea del negocio; y
4. Completas: ejecución de todos los planes y procedimientos de recuperación de la organización completa. Evaluación de las capacidades alternas de operación en un ambiente altamente estresado. Eventualmente, se podría involucrar a las entidades del sector público competentes.
5. Las pruebas que la entidad realice podrán ser parciales, controladas, temporales y no anunciadas, hasta pruebas completas de escenarios de interrupción que involucren la participación de agentes externos, principalmente de los proveedores de servicios críticos. Para una ejecución ordenada, la entidad establecerá un programa de pruebas que deberá ejecutarse en la misma periodicidad establecida en el presente artículo.

Las entidades, con al menos 30 días de antelación, deberán informar a la Superintendencia sobre el tipo y fecha de realización de las pruebas a que hace referencia el presente artículo, pudiendo requerir a la Superintendencia presenciar la realización de las mismas.

1. En todos los casos, las pruebas deben tener objetivos definidos y producir estimaciones de los MPTD, OMCN, POR y TOR, realizadas por el personal responsable de los procesos críticos de la entidad, así como un reporte detallado de los resultados alcanzados y las recomendaciones, detallando la fecha, hora de inicio y fin, responsables de las actividades, errores detectados y fallas en las pruebas. Esta información será básica para la actualización del plan de continuidad del negocio.

**CAPÍTULO V**

**OTRAS DISPOSICIONES Y VIGENCIA**

**Tercerización**

1. La tercerización o servicios críticos provistos por terceros se enmarcarán dentro de la gestión de los riesgos operacionales, debiendo las entidades establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los servicios críticos brindados por terceros. Las entidades deben verificar que las empresas proveedoras de servicios críticos mantengan los criterios de continuidad del negocio de la entidad en cumplimiento de las presentes Normas y al Anexo No. 1 de las Normas Técnicas sobre la Gestión de la Seguridad de la Información, que emita el Banco Central por medio de su Comité de Normas.

En el contrato deberá constar todo lo que aplique conforme a las normas vigentes, entre ellos, que no exista restricción alguna por parte del proveedor para que la Superintendencia pueda realizar las evaluaciones que considere pertinentes para supervisar que los servicios para los que el proveedor ha sido contratado cumplen con los criterios de continuidad del negocio, así como con el marco legal y normativo aplicable a la entidad contratante.

Adicionalmente, la entidad debe contar con la documentación que sustente la concientización, capacitación, plan de continuidad, pruebas desarrolladas y los resultados de las pruebas efectuadas en las empresas tercerizadoras o con la participación de ellas.

**Documentación de respaldo**

1. Las entidades deben mantener a disposición de la Superintendencia la documentación que permita sustentar el desarrollo de cada una de las etapas o actividades descritas en el artículo 9 de las presentes Normas, como parte del informe anual de la gestión de los riesgos operacionales.

**Cambios significativos**

1. Las entidades analizarán el impacto que tienen los cambios significativos sobre la continuidad del negocio. Los cambios significativos que se podrán considerar, entre otros, son: cambios de la infraestructura tecnológica que soportan los productos o servicios prioritarios, fusión con otra entidad, implementación de un nuevo producto, servicio o canal de servicio, cambio de un proveedor o cambio de oficina principal.

**Auditoría Interna**

1. La Unidad de Auditoría Interna debe considerar en su plan anual de trabajo la evaluación del cumplimiento de las disposiciones establecidas en las presentes Normas.

**Plan de Adecuación**

1. Las entidades, para cumplir las disposiciones establecidas en las presentes Normas, deberán presentar a la Superintendencia un plan de adecuación, dentro de los treinta días siguientes a la vigencia de las presentes Normas. Una vez presentado el plan, las entidades deberán implementarlo en un plazo máximo de once meses contados a partir de su presentación.

**Sanciones**

1. Los incumplimientos a las disposiciones contenidas en las presentes Normas, serán sancionados de conformidad con lo previsto en la Ley de Supervisión y Regulación del Sistema Financiero.

**Aspectos no previstos**

1. Los aspectos no previstos en temas de regulación en las presentes Normas serán resueltos por el Banco Central, por medio de su Comité de Normas.

**Vigencia**

1. Las presentes normas entrará en vigencia a partir del día XX de XXXX del dos mil diecinueve.