PO-072-0

POLÍTICA SISTEMA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

MANUAL

SISTEMA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

SUBPROCESO

SISTEMA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Aprobaciones	
Dueño de Proceso: Giovanny Oswaldo Bautista Marulanda	Helber Alonso Melo Hernández
Cargo: Gerente de Ciberseguridad, Seguridad de la Información, Privacidad y Continuidad (E)	**Cargo:** Vicepresidente de Riesgos

1 INTRODUCCIÓN

La Gestión de Riesgos de Continuidad de Negocio constituye un pilar fundamental para el adecuado cumplimiento del objeto social del Banco. Como parte de las responsabilidades previstas en normas legales y reglamentarias las entidades sometidas a inspección y vigilancia por parte de la SFC, deben Implementar, probar y mantener un proceso para administrar la continuidad de la operación de la entidad, que incluya elementos como: prevención y atención de emergencias, administración y comunicación en crisis, planes de contingencia para responder a las fallas e interrupciones específicas de un sistema o proceso, y capacidad de retorno a la operación normal[1].

2 OBJETIVO

Definir los lineamientos generales, para la adecuada implementación y mantenimiento del Sistema de Gestión de Continuidad de Negocio (SGCN) del Banco Popular, con el fin de asegurar la ejecución de las operaciones en sus actividades esenciales y críticas en caso de una interrupción del negocio.

2.1 OBJETIVOS ESPECIFICOS

- Establecer las directrices generales, para que las áreas identificadas con subprocesos críticos implementen y mantenga los elementos que conforman el SGCN.

- Realizar seguimiento al estado de los eventos de Continuidad de Negocio presentados y de las acciones de mitigación o planes de acción adoptados por parte de los dueños de proceso identificados como críticos.

- Propender por la definición de un sistema de medición del SGCN que permita contar con un diagnóstico del estado del mismos y contribuya en la adopción de mejoras al sistema.

- Adoptar o implementar las herramientas suministradas por el SGCN.

- Fortalecer el compromiso de la Alta Gerencia en el Banco, impartiendo lineamientos para el apoyo en la gestión y mantenimiento del Sistema de Gestión de Continuidad de Negocio.

[1] Numeral 4.2.6 Parte I, Título I, Capítulo IV Circular Básica Jurídica 029 de 2014 expedida por la Superintendencia Financiera de Colombia.

3 ALCANCE

La presente política y las directrices consignadas en este documento constituyen el marco de gobierno del Sistema de Gestión de Continuidad de Negocio - SGCN del Banco Popular, y se establece como una herramienta de consulta permanente para todas las áreas del Banco, en especial de las áreas identificadas con subprocesos críticos. Es responsabilidad de los empleados directos y trabajadores en misión, cumplir con lo establecido en este documento.

4 DECLARACIÓN DE COMPROMISO

El Banco Popular se compromete a honrar los compromisos adquiridos con sus accionistas, clientes, colaboradores, proveedores, entidades del Estado y entes reguladores, los cuales se pueden ver comprometidos por incidentes, emergencias, desastres y crisis que causen una interrupción en la operación de los procesos y prestación de sus servicios y que pongan en riesgo su estabilidad, a través de estrategias y planes de continuidad de negocio que le permita afrontar de manera satisfactoria estas situaciones; para lo cual cuenta con la participación y compromiso de todos y cada uno de los colaboradores del Banco.

5 LINEAMIENTOS GENERALES

5.1 LINEAMIENTO DEL BANCO POPULAR DE LA CONTINUIDAD DE NEGOCIO

La Alta Dirección del Banco Popular reconoce la importancia de contar con un Sistema de Gestión de Continuidad de Negocio, el cual permite responder adecuadamente a eventos de indisponibilidad y mantener la resiliencia de la entidad ante dichas situaciones. Por lo anterior, el Banco define, implementa, prueba y mantiene un proceso para administrar la Continuidad de Negocio, incluyendo elementos como: prevención y atención de emergencias, administración de escenarios de crisis, comunicación en crisis, planes de contingencia y capacidad de retorno a la operación normal, de acuerdo con su estructura, tamaño, objeto social y actividades de apoyo. La gestión del SGCN, fortalece la cultura de continuidad de negocio permitiendo la adopción por parte de los colaboradores del Banco, funcionarios temporales y proveedores que en el ejercicio de sus funciones participen en la operación critica de las compañías; por lo anterior, el Banco Popular en esta política debe velar por:

- El cumplimiento de lineamientos y principios de continuidad de negocio.
- La adopción de buenas prácticas tales como, ISO 22301, las prácticas profesionales del DRII, PAS200, ISO 27031, entre otras.
- Administrar, gestionar y mitigar los riesgos de indisponibilidad en los procesos críticos de la organización.

- Establecer y divulgar las directrices, normas, políticas, estándares, procedimientos e instructivos de continuidad de negocio, generando compromiso en todas las áreas de la organización.
- Fortalecer la cultura de continuidad de negocio.
- Considerar dentro del Plan de Continuidad de Negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos y los demás escenarios definidos al interior de la compañía de acuerdo contexto de esta.
- Realizar pruebas del Plan de Continuidad de Negocio que simulen la materialización de ataques cibernéticos y demás escenarios contemplados en la construcción del plan de continuidad de negocio y establecimientos de estrategias de recuperación.
- Contar con un comité de continuidad de negocio que se constituya en el órgano técnico de asesoría a la Alta Dirección. Los miembros que hagan parte de este comité deben tener conocimiento y experiencia en la administración de riesgos asociados a indisponibilidad y desarrollo de estrategias de continuidad de negocio.
- Proveer los recursos necesarios para el mantenimiento del Sistema de Gestión de Continuidad de Negocio - SGCN.
- Remitir a Grupo Aval los informes que esta requiera respecto de continuidad de negocio.
- Revisar las herramientas tecnológicas usadas en el mercado para la administración de la continuidad de negocio y así de acuerdo con las bondades de estas, sugerir la adopción corporativa.
- Los nuevos procesos relacionados con la operación de los productos y servicios que se incorporen al Banco deben contemplar desde su inicio la implementación de la política de continuidad de negocio.
- La responsabilidad de mantener la continuidad de los servicios y procesos críticos es parte integral del desarrollo de las actividades que desempeña cada uno de los colaboradores del Banco, y en especial los cargos con responsabilidades directas en los planes de recuperación de procesos.
- Todo cambio operacional, estratégico, tecnológico, institucional y de infraestructura física en el Banco Popular, requiere la actualización de la evaluación de riesgo, el análisis de impacto y la documentación que soporta el Sistema de Gestión de Continuidad de Negocio, en adelante, “SGCN”, validando la suficiencia de la estrategia de recuperación y continuidad frente a los resultados obtenidos.
- Las estrategias de continuidad y recuperación están alineadas con las políticas y lineamientos de operación interna del Banco (SARO, Seguridad de la Información, SARLAFT, entre otros).
- Desarrollar y mantener vigentes las estrategias de mitigación y respuesta ante eventos de interrupción, desastre o emergencia, de forma tal que el Banco tenga la capacidad de reaccionar adecuada y oportunamente.

- Desarrollar y mantener vigentes los diferentes planes que conforman el SGCN del Banco, tales como:

- Planes de recuperación de los procesos críticos, a cargo de cada dueño de proceso - Gerente Dirección General
- Plan de recuperación ante desastres, a cargo de la Gerencia de Operaciones de Tecnología
- Planes de emergencia, a cargo de la Gerencia de Atención y Servicios al Talento Humano
- Plan de comunicación de crisis a cargo de la Gerencia de Experiencia de Marca.
- Plan de administración de crisis, a cargo de la Vicepresidencia de Riesgos.

Definir y mantener vigente la definición de roles, responsabilidades y la estructura de respuesta necesaria para enfrentar adecuadamente eventos de interrupción, desastre, crisis o emergencia que puedan afectar los procesos, operaciones y servicios críticos del Banco.

Acorde con lo anterior, Banco Popular acoge las siguientes políticas sobre las cuales se fundamenta y estructura el Sistema de Gestión de Continuidad de Negocio (SGCN).

Siendo así y bajo los parámetros principales del SGCN se deben tener en cuenta al menos los siguientes lineamientos.

5.2 GESTIÓN DE RIESGOS

- Validar que los riesgos asociados a la continuidad de negocio estén homologados dentro del catálogo de riesgos genéricos, los cuales están definidos bajo los lineamientos establecidos en los comités corporativos de Grupo Aval con las entidades.
- Medir y evaluar riesgos de indisponibilidad de infraestructura tecnológica, recurso humano, infraestructura física y proveedores. Para el caso de registros vitales, verificar contra las matrices de activos de información en las cuales se evalúa el criterio de disponibilidad y que ameriten una estrategia de continuidad.
- Validar periódicamente que los riesgos de continuidad de negocio estén documentados y actualizados en las matrices de riesgo de la entidad y se encuentren dentro de los límites de apetito, tolerancia y capacidad establecidos.

5.3 ANÁLISIS DE IMPACTO AL NEGOCIO

- Establecer y actualizar los procesos críticos que son del alcance de continuidad de negocio, a través de un análisis de impacto – BIA, mínimo una vez al año o cuando se requiera.
- En la valoración de los procesos críticos, se deben tener en cuenta aspectos como los acuerdos de servicio al cliente, cumplimientos con entes regulatorios y terceros que apoyen parte de la operación de los procesos críticos del Banco.

- La Alta Dirección o el comité que se disponga en la entidad, debe validar los resultados del BIA y quedar su aprobación mediante acta.

5.4 ESTRATEGIAS DE RESPUESTA

- Establecer estrategias de respaldo y recuperación para los procesos críticos identificados.
- Garantizar que el tiempo de recuperación objetivo (RTO) y el punto objetivo de recuperación (RPO) sean acordes con las necesidades del negocio. Así mismo cuando los servicios tecnológicos no son administrados directamente por la entidad.
- Mantener niveles óptimos de seguridad en los ambientes de producción y contingencia, de acuerdo con su modelo en cada ambiente.
- Incluir en el presupuesto anual la adquisición de recursos para la sostenibilidad del SGCN, tanto para mantenimiento e implementación de estrategias como de formación del equipo de continuidad.
- Documentar las estrategias de continuidad y contingencia, las cuales deben estar soportadas en manuales o procedimientos, que identifiquen claramente la recuperación del personal, infraestructura tecnológica, infraestructura física, proveedores y demás recursos que se consideren necesarios, en procura de permitir su buen funcionamiento en el antes, durante y después de una interrupción.
- Las estrategias deben estar encaminadas a cumplir con las fases de respuesta, recuperación, reanudación de la operación en contingencia y restauración de los diferentes escenarios de indisponibilidad identificados en la entidad.
- Participar de los proyectos en las entidades que puedan tener efecto sobre el SGCN.

5.5 PLAN DE GESTIÓN DE CRISIS

- Elaborar e implementar el plan de gestión de crisis que contenga actividades desde la atención, gestión, escalamiento y manejo de incidentes o eventos de crisis.
- Incluir en el cronograma de pruebas anual, el despliegue de las estrategias para el funcionamiento de los centros de comando o salas de crisis, la estrategia debe contar con salas de crisis físicas y/o virtuales que permitan desplegar comunicación entre la alta dirección de manera efectiva.
- Definir los procedimientos y protocolos de comunicación, que incluyan entre otras, los voceros autorizados de la entidad ante eventos de crisis, mensajes predeterminados de acuerdo con los escenarios que aplique, los medios por los cuales se va a comunicar y las audiencias.
- Fortalecer la cultura en continuidad de negocio para que al interior de la entidad todo el personal conozca sus roles y responsabilidades en los protocolos definidos para el manejo de crisis.
- Cuando se presenten eventos de crisis, deben ser comunicados por el Vicepresidente de Riesgos a la Vicepresidencia de Riesgos Corporativos de Aval.
- Verificar que se establecen, prueban y actualizan los árboles de llamadas.
- Contar con medios efectivos para la actualización permanente de los datos de contacto, con el fin de emitir comunicados internos en el tiempo adecuado.

- Los árboles de llamadas deben ser incluidos en el plan de pruebas anual.

5.6 PLAN DE EMERGENCIAS

El Banco debe establecer y generar destrezas, condiciones y procedimientos que les permita a los ocupantes de las instalaciones de la Entidad, protegerse en caso de desastres o amenazas colectivas y prevenir situaciones que puedan poner en peligro su integridad. Para el efecto se debe contar con un Plan de Emergencia, el cual deberá estar enmarcado bajo los siguientes lineamientos:

- Integrar ejercicios de emergencia con las estrategias de continuidad.
- Realizar por lo menos un simulacro anual.
- Mantener permanente comunicación entre el líder de continuidad y el líder de emergencias con el fin de valorar el alcance y despliegue de estrategias, de acuerdo con inputs tales como el análisis de riesgos efectuado de parte y parte.

5.7 PLAN DE RECUPERACIÓN DE DESASTRES DRP

- Las entidades deben contar con un DRP debidamente establecido y documentado, que garantice el restablecimiento de los procesos críticos de la entidad y los de apoyo que los soportan dentro de los tiempos de recuperación definidos en el Plan de Continuidad de Negocio (PCN).
- Las entidades deben contar con un CAPD (centro alterno de procesamiento de datos) y los respaldos que necesite para apoyar el plan de Continuidad de Negocio.
- Las entidades deben tener definidos y asignados los roles y responsabilidades para la administración, gestión y operación del DRP.
- El CAPD debe responder a las necesidades críticas del negocio, identificadas en el BIA que la entidad haya desarrollado.
- El CAPD debe estar disponible para recuperar los servicios críticos del negocio dentro de los tiempos RTO y RPO definidos en el BIA.
- En el BIA se deben establecer los procesos críticos y como resultado, debe servir de insumo para la secuencia de recuperación de los servicios críticos. Dicho resultado, debe ser acorde con el evento que se presente y en línea con los escenarios de contingencia y de ciberseguridad que la entidad define en su Plan de Continuidad de Negocio.
- El CAPD debe operar y prestar la totalidad de los servicios críticos definidos en el BIA, con total independencia del CPD.
- El alcance y la capacidad de los servicios de tecnología implementados en el CAPD deben responder a las necesidades del negocio documentadas en el BIA.
- Toda la infraestructura de TI instalada en el CAPD debe ser monitoreada y gestionada por la Entidad.
- Se puede usar el CAPD para funciones diferentes a la Recuperación de Desastres (DR), sin embargo, el responsable del DRP debe garantizar que, al presentarse una

contingencia parcial o total, el CAPD esté disponible en el tiempo para cumplir con el RTO.

- El CAPD debe incluir en su diseño una estrategia que le permita tener puntos de recuperación de la operación. Esta estrategia incluye archivos de configuración de toda la infraestructura instalada y datos de los procesos críticos. En detalle los puntos de recuperación son copias de la información con tiempos definidos por la entidad para activar una configuración o datos “sanos” de los procesos críticos en caso de corrupción de la data en producción y contingencia. Son copias o algún sistema de respaldo con minutos de retraso.
- La información de la configuración de toda la infraestructura del CAPD (almacenamiento, procesamiento, redes lógicas y eléctricas), debe ser actualizada cada vez que se realice un cambio, y tener puntos de recuperación acorde con las necesidades del negocio.
    - Cada nuevo proyecto de implementación de un servicio del negocio que involucre servicios de TI debe valorarse y determinar si es crítico, en cuyo caso se requiere implementación en el CAPD, y este debe estar implementado y probado antes de iniciar el servicio en producción.
- La información de los puntos de recuperación de la infraestructura debe estar almacenada en sitios seguros diferentes a los centros de procesamiento de datos y de fácil acceso para los responsables de dicha información.
- Cada servicio implementado en el CAPD debe tener las mismas características de seguridad informática (hardware y software) que las del CPD.
- En caso de que el RTO de un servicio se vea afectado por la aplicación de las medidas de seguridad, la entidad decide el nivel de riesgo que asume para cumplir con el RTO. Las medidas de seguridad hacen referencia a todos los sistemas y controles de seguridad informática que se tienen implementados en el CPD, y que al momento de pasar a contingencia no se cuenten con los mismos, ejemplos: fallas en los tokens de acceso remoto y que se requiera acceder con solo usuario y contraseña.
- La infraestructura del CAPD debe ser actualizada cada vez que se realice un cambio o implementación de un servicio crítico en el Centro Principal de Procesamiento de Datos (CPD). Las actualizaciones deben ser autorizadas por el Comité de Cambios de la Entidad.
- El responsable del DRP o un colaborador que integre el equipo del DRP, debe participar en el Comité de Cambios, para verificar y alertar posibles riesgos e impactos que puede generar los cambios propuestos.
- Cada cambio en el DRP debe ser probado en el CAPD, cuando se modifiquen servicios en producción y alcancen también servicios compartidos entre varias entidades o terceros.
- Se deben procurar realizar pruebas totales con atención a usuarios/clientes por lo menos 1 vez al año, en todo caso los cronogramas de pruebas de las entidades deben contemplar obligatoriamente pruebas integrales y parciales.
- Se debe mantener actualizada y disponible la documentación del DRP (Análisis de Riesgos, BIA, estrategia, planes y resultados de pruebas) en un sitio alterno con una estrategia de contingencia, el cómo o detalle de la estrategia lo define cada entidad, pero el lineamiento es que cada entidad ante la indisponibilidad de su CPD pueda

tener acceso a la información sin problema alguno para activar su Plan de Continuidad de Negocio.

- Toda la documentación de DRP, debe ser revisada y actualizada al menos una vez por año, y cada vez que un nuevo servicio del negocio se implemente en el CADP.
- El responsable del DRP debe generar informes internos del estado del CAPD donde la Entidad tenga la verificación de que el DRP está monitoreado, es funcional y puede ser activado en cualquier momento, para entrar a operar en caso de contingencia. Es importante que las entidades validen periódicamente en el DRP los cambios de configuraciones, actualizaciones, cambios de usuarios, contraseñas, sincronizaciones entre otros, para que los ambientes en el CPD y el CAPD, estén permanentemente actualizadas cada que se haga una modificación en producción.
- La entidad debe generar mensualmente el estado del DRP al menos bajo la siguiente estructura. Dicho informe podrá ser consultado por Grupo Aval de acuerdo con el consumo de información que se acuerde con cada entidad.

El reporte debe como mínimo contener los siguientes elementos:

- Servicios de TI que soportan los procesos críticos definidos en el BIA.
- Disponibilidad de cada uno de los servicios.
- Capacidad de cada servicio.
- Confirmación de los tiempos de activación de los servicios en caso de presentarse un incidente (RTO).
- Confirmación de que se cuenta con la información necesaria para reactivar los servicios (configuraciones y Datos) con los RPO definidos o puntos de recuperación.

5.8 CAPACITACIÓN Y SENSIBILIZACIÓN

El Banco debe mantener en vigencia un programa permanente de creación y mejoramiento de cultura en continuidad de negocio, que resalte la importancia del cumplimiento del Sistema de Gestión de Continuidad de Negocio.
Este programa debe ser realizado desde el mismo momento del ingreso de un colaborador (inducción) y una vez al año o cuando se requiera a los involucrados en el Sistema de Gestión de Continuidad de Negocio de cada Entidad.

El programa debe contemplar como mínimo los siguientes elementos:

- Capacitaciones especializadas para cada equipo que haga parte del Plan de Continuidad de Negocio.
- Evaluaciones periódicas de los resultados del programa de concientización a fin de medir su efectividad y obtener información que permita establecer ajustes y correctivos en su diseño y ejecución.
- Planes de capacitación para el personal encargado de administrar el SGCN.

5.9 GESTIÓN DE RIESGOS DE PROVEEDORES

El Banco debe realizar control y seguimiento a los planes de continuidad de los terceros críticos, además sensibilizarlos respecto del nivel de criticidad para la ejecución de los procesos, para esto deben por lo menos atender los siguientes lineamientos:

- Identificar los proveedores críticos de los procesos a través de la metodología interna que use la entidad, pero dejando registro en el Análisis de Impacto al Negocio (BIA).
- Los contratos de los terceros críticos deben incluir cláusulas de cumplimiento frente a la implementación y mantenimiento del Plan de Continuidad de Negocio por parte del tercero, estas cláusulas serán incluidas para los casos que aplique donde la contratación sea exclusiva de un servicio por parte de la entidad, no aplica para adhesión a consumo de servicios prestados a nivel de mercado.
- Para los terceros críticos, contar con garantías suficientes de continuidad de negocio a través de certificación de su plan de continuidad y cláusulas contractuales. En todo caso, requerir las contingencias a que haya lugar en caso de indisponibilidad de los servicios por parte del tercero.
- Evaluar anualmente el estado de preparación en continuidad de negocio de acuerdo con su criticidad (metodología interna), a través de alguna de las siguientes actividades:

  - Visitas a las instalaciones del proveedor (presencial o virtual).
  - Solicitud de certificación del estado de implementación del Plan de Continuidad de Negocio o ejecución de pruebas de continuidad.

  En los casos que sea posible y que la entidad así lo considere, acompañar la ejecución de las pruebas de continuidad de los servicios que prestan los proveedores críticos a la Entidad, teniendo en cuenta los niveles de criticidad mayores o extremos.

- A través del comité corporativo de continuidad de negocio, presentar para evaluación el seguimiento o visita a un proveedor y que pueda servir a otras entidades del grupo para su cumplimiento. Valorar si desde este comité se puede invitar al proveedor de interés común para que exponga el PCN en una sesión y sirva como certificación para el Grupo de entidades.
- Emitir anualmente o cuando se actualice, listado de proveedores críticos a Grupo Aval, en el cual se identifique el NIT, nombre, descripción del servicio contratado, proceso critico asociado. En caso de tener más de un contrato se debe enviar la información de todos los servicios críticos.

5.10 PRUEBAS Y EJERCICIOS

El Banco debe realizar ejercicios y pruebas de sus procedimientos de continuidad de negocio para asegurar que las estrategias sean consistentes con los objetivos del negocio. Además, contar con la realización de pruebas de los diferentes planes del sistema, donde se evidencie la prueba del producto o proceso + DRP (en conjunto o independientes), emergencia, planes de comunicación y administración de crisis.

El Banco debe realizar las pruebas teniendo en cuenta los siguientes lineamientos:

- Realizar al menos una prueba integral en el año donde se incluya el despliegue de estrategias de centro(s) alterno(s) de operaciones y centro alterno de procesamiento de datos.
- Cuando sea posible por el nivel de madurez del SGCN, realizar pruebas con los procesos críticos en horario hábil.
- Medir tanto a nivel tecnológico como funcional la ejecución de las pruebas.
- En el plan de pruebas anual indicar el tipo, alcance y objetivos generales de las pruebas a realizar, lo mismo que las fechas y áreas involucradas.
- En lo posible ejecutar pruebas de continuidad que integren planes de emergencia y de administración y comunicación en crisis.
- Realizar pruebas del Plan de Continuidad de Negocio que simulen la materialización de ataques cibernéticos.
- Hacer seguimiento a la atención de oportunidades de mejora identificadas durante las pruebas y verificar su cumplimiento.

5.11 HERRAMIENTA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO

El Banco de acuerdo con su nivel de madurez sobre el SGCN podrán optar por la adopción de una herramienta tecnológica que permita gestionar las actividades que comprenden la preparación, respuesta, recuperación, restauración, reanudación.
Por lo anterior y en lo posible, la herramienta podrá ser a nivel corporativo para facilitar su agregación de datos.

5.12 INFORMACIÓN Y COMUNICACIÓN

Comunicación de los resultados de la gestión de SGCN:

- Informar a la Junta Directiva (JD) o Comité de Auditoría (CA) y/o Comité de Continuidad de Negocio quien haga sus veces, los escenarios de crisis o catastróficos y sus correspondientes estrategias de recuperación en la Entidad, resultados de pruebas y ejercicios, eventos de alto impacto e información relevante del SGCN.

- Asegurar la oportunidad, pertinencia y calidad de la información, remitida a Grupo Aval.

5.13 MONITOREO DEL SGCN

La entidad debe realizar seguimiento y monitoreo a los diferentes componentes del SGCN, con el fin de identificar brechas frente a su ejecución y operación, para lo anterior, la entidad a pesar de sus procesos de monitoreo internos debe consolidar y evaluar anualmente su Sistema de Gestión a partir del modelo de madurez definido a nivel corporativo.

6 ESTRUCTURA DE GOBIERNO

El gobierno de continuidad de negocio establece las líneas de interacción y trabajo en equipo requerido para asegurar una preparación efectiva ante situaciones de crisis, desastre o interrupción. Teniendo en cuenta la necesidad de disponer y asignar funciones específicas en el Banco Popular para la Gestión de Continuidad del Negocio, de forma tal que se pueda dar sostenibilidad y mantenimiento permanente al estado de preparación del Banco, se establece la siguiente estructura responsable de la gestión del sistema de continuidad:

Roles y responsabilidades en la planeación y preparación en continuidad del negocio.

6.1 LÍNEAS DE DEFENSA FRENTE A LA GESTIÓN DEL RIESGOS

El Banco Popular debe estructurar las funciones y responsabilidades frente al Riesgo de Continuidad de Negocio, de acuerdo con la Política Corporativa para la Gestión Integral de Riesgos; este marco de referencia define el esquema de las tres líneas de defensa considerando (i) la gestión por la línea de negocio, (ii) una función de Gestión de Continuidad de Negocio independiente, y (iii) una revisión independiente.

6.1.1 Primera Línea de Defensa

La primera línea de defensa la constituyen los procesos y todos los colaboradores del Banco Popular. La Política de Continuidad de Negocio reconoce a los diferentes procesos (Dueños de proceso y los colaboradores a cargo) como responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos e incidentes de continuidad de negocio inherentes a los productos, servicios, procesos y sistemas. Quienes conforman esta línea de defensa deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas. Se excluye la gestión de riesgos y la Contraloría Interna.

6.1.2 Segunda Línea de Defensa

Esta línea de defensa está conformada por la Vicepresidencia de Riesgos, la cual debe establecer los lineamientos en esta materia y realizar un seguimiento continuo al cumplimiento de todas las obligaciones de continuidad de negocio. El líder de continuidad de negocio deberá contar con alto nivel jerárquico para proponer las estrategias de continuidad y contingencia idóneas para la respuesta a eventos de indisponibilidad, además con suficientes atributos para convocar al comité de crisis. Es responsable de presentar los resultados de gestión directamente a la Alta Gerencia o al Comité de Auditoría. Así mismo, debe contar con recursos suficientes para realizar eficazmente todas sus funciones y desempeñar un papel central y proactivo en el Sistema de Gestión de Continuidad de Negocio. Para ello, debe estar plenamente familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentarios y los riesgos de continuidad de negocio derivados de la operación de la entidad.

6.1.3 Tercera Línea de Defensa

La tercera línea es responsable de evaluar de forma independiente la gestión y los controles de los riesgos de continuidad de negocio, así como las políticas, estándares y procedimientos de los sistemas, rindiendo cuentas al Comité de Auditoría. Las personas encargadas de auditorías internas que deben realizar estas revisiones deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control. Esta revisión puede ser realizada por el personal de auditoría, pero también puede involucrar actores externos debidamente calificados.

6.2 JUNTA DIRECTIVA

Sin perjuicio de las funciones asignadas en otras disposiciones es responsabilidad de la Junta Directiva u órgano que haga sus veces:

- Aprobar la política del Sistema de Gestión de Continuidad del Negocio y sus modificaciones.
- Proveer los recursos necesarios para desarrollar y actualizar en forma permanente el Sistema de Gestión de Continuidad de Negocio (Diseño, implementación, capacitación y pruebas).
- Pronunciarse respecto a los informes periódicos relacionados con el Sistema de Gestión de Continuidad del Negocio, que presente el Vicepresidente de Riesgos.
- Impartir, cuando lo considere pertinente, las directrices para el mejoramiento de la Gestión de Continuidad de Negocio.

6.3 COMITÉ DE RIESGOS NO FINANCIEROS

Las responsabilidades del Comité de Riesgos No Financieros están definidas en la POLÍTICA SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS, Numeral 7.2.1 Comités de Riesgo Especializados, y las mismas son aplicables al Sistema de Gestión de Continuidad de Negocio.

6.4 COMITÉ DE AUDITORÍA

- Apoyar a la Junta Directiva en el seguimiento al Sistema de Control Interno de la entidad en lo que tiene que ver con el Sistema de Gestión de Continuidad de Negocio - SGN
- Evaluar y hacer seguimiento a los informes resultado de las auditorías realizadas al Sistema de Gestión de Continuidad de Negocio - SGCN
- Pronunciarse sobre la evaluación periódica de continuidad de negocio, que realicen los órganos de control.

6.5 COMITÉ CORPORATIVO DE CONTINUIDAD DE NEGOCIOS (GRUPO AVAL Y ENTIDADES)

Este comité sesionará bimestralmente, está conformado por Grupo AVAL Holding y sus principales entidades, Banco de Bogotá, Banco de Occidente, Banco Popular, Banco AV Villas, BAC Credomatic, la Corporación Financiera Colombiana (Corficolombiana), la Administradora de Fondos de Pensiones y Cesantías (Porvenir), ATH y NEXA BPO, con las siguientes funciones principales:

- Participar activamente en la definición y actualización de las políticas y lineamientos del SGCN, establecer consenso sobre las mismas para la aprobación por parte de la Vicepresidencia de Riesgos Corporativos de Grupo AVAL.
- Proponer para su aprobación por parte de la Vicepresidencia de Riesgos Corporativos de Grupo AVAL, la Política Corporativa de Continuidad de Negocio.
- Determinar y revisar, cuando se requiera, las políticas generales del Sistema de Gestión de Continuidad de Negocio (SGCN).
- Analizar los SGCN implementados en las entidades financieras del Grupo.
- Definir el cronograma de reuniones a realizar durante el año vigente para informar las novedades del SGCN en cada entidad.
- Revisar temas regulatorios que puedan afectar al SGCN y darlos a conocer para tomar medidas de aplicación.
- Establecer lineamientos de mejora al SGCN
- Compartir las buenas prácticas utilizadas en el mercado.
- Ser el canal táctico de seguimiento, monitoreo y control del conglomerado a las entidades.
- Valoración anual del catálogo de riesgos y controles genéricos asociados al SGCN.

6.6 COMITÉ DE CONTINUIDAD DE NEGOCIO DEL BANCO

Este Comité está compuesto por:

- Vicepresidencia de Riesgos.
- Vicepresidencia de Tecnología.
- Gerencia TI de Operaciones y Servicios de Tecnología.
- Gerencia de Experiencia, Marca y Sostenibilidad.
- Gerencia de Abastecimiento Estratégico.
- Gerencia de Ciberseguridad, Seguridad de la Información, Privacidad y Continuidad.
- Gerencia de Gestión y Desarrollo del Talento Humano.
- Gerencia de Atención y Servicio al Talento Humano.
- Gerencia de Comunicaciones.
- Dirección de Continuidad de Negocio.
- Dirección de Confiabilidad Operativa de Tecnología y DRP.
- Director de Seguridad y Salud en el Trabajo.
- Director de Infraestructura.

Podrán ser invitadas Vicepresidencias, Gerencias o Personas que se consideren necesarias, dependiendo de los temas a tratar.

Este comité tiene como finalidad verificar que el SGCN funcione de manera efectiva, se reunirá trimestralmente o cuando se requiera y sus funciones son:

- Contribuir en la definición de los lineamientos generales y la estructura del SGCN, así como efectuar el seguimiento y evaluar la efectividad del mismo.
- Supervisar las actividades del SGCN con el objeto de verificar que su alcance satisface las necesidades de la Entidad.
- Generar alertas y recomendaciones que permitan establecer oportunidades de mejora al SGCN.
- Evaluar los planes de trabajo, los informes y dar seguimiento al cumplimiento de las recomendaciones.
- Apoyar el proceso de implementación de estrategias de continuidad de negocio.
- Supervisar el nivel de madurez del SGCN y realizar seguimiento a los indicadores de medición
- Verificar el cumplimiento de las políticas establecidas en el SGCN a través de los resultados de las diferentes auditorías, evaluaciones y pruebas que se le realicen al sistema.
- Evaluar el nivel de cubrimiento del SGCN a nivel de procesos, servicios, productos y operaciones críticas del Banco.

6.7 VICEPRESIDENCIA DE RIESGOS

La Vicepresidencia de Riesgos, es responsable de liderar las definiciones sobre el Sistema de Gestión de Continuidad de Negocio, tales como estructura metodológica, políticas, roles, responsabilidades, entre otras. Las funciones a su cargo son:

- Liderar, articular y monitorear el desempeño del SGCN conforme a las políticas internas definidas y la normatividad vigente aplicable.
- Liderar el desarrollo, implementación y actualización del SGCN para asegurar su efectividad y sostenibilidad.
- Convocar el Comité de Administración de Crisis.
- Participar en el Comité de Administración de Crisis.
- Participar y liderar el Comité de Continuidad de Negocio.
- Gestionar que las políticas, instructivos, lineamientos y demás documentos que son suministrados por Grupo Aval sean de uso restringido al personal de la entidad y sus filiales y subsidiarias, de modo que las personas que tengan acceso a estos documentos sean las responsables de la custodia y la conservación.

6.8 GERENTE DE CIBERSEGURIDAD, SEGURIDAD DE LA INFORMACIÓN, PRIVACIDAD Y CONTINUIDAD

El Gerente de Ciberseguridad, Seguridad de la Información, Privacidad y Continuidad es el responsable de:

- Gestionar el SGCN mediante herramientas y metodologías para el cumplimiento de las políticas y procedimientos establecidos por la Entidad.
- Convocar el Comité de Continuidad de Negocio.
- Liderar, velar por cumplimiento y el correcto desempeño del plan de recuperación de procesos – BCP, conforme a las políticas internas definidas y la normatividad vigente aplicable.
- Implementar las acciones que permitan la efectividad y sostenibilidad del BCP y los elementos que lo componen.
- Gestionar el presupuesto para el plan de recuperación de procesos – BCP.
- Definir y gestionar los programas de capacitación sobre el plan de recuperación de procesos – BCP.
- Monitorear la implementación de las estrategias de continuidad definidas para el Plan de Recuperación de Procesos – BCP.
- Realizar seguimiento a la definición de planes de acción en los eventos de indisponibilidad de alto impacto y/o relevantes.
- Realizar seguimiento a la definición de planes de acción resultado de las evaluaciones efectuadas por la tercera Línea de Defensa.
- Reportar a Grupo Aval los eventos de riesgo de alto impacto y/o relevantes que se materialicen.
- Evaluar mínimo anualmente, a través del modelo de madurez corporativo el SGCN.

- Asegurar el acompañamiento de personal especializado y que se considere necesario, durante las visitas que se realicen de parte de Grupo Aval y que estén relacionadas con la continuidad de negocio.
- Participar en las sesiones programadas por Grupo Aval del Comité Corporativo de Continuidad de Negocio.
- Gestionar la adopción de los lineamientos impartidos por Grupo Aval.
- Compartir las buenas prácticas utilizadas en el mercado.
- Requerir planes de acción y realizar seguimiento a desviaciones presentadas en el Sistema de Gestión de Continuidad de Negocio - SGCN
- Seguir los lineamientos establecidos por el Comité Corporativo de Continuidad de Negocio.

6.9 DIRECTOR DE CONTINUIDAD DE NEGOCIO

El Director de Continuidad de Negocio, de la Gerencia de Ciberseguridad, Seguridad de la Información, Privacidad y Continuidad, es el responsable de coordinar la implementación, pruebas y actualizaciones sobre el Sistema de Gestión de Continuidad de Negocio, y debe asegurar el uso, entendimiento y divulgación de la estructura metodológica, políticas, roles y responsabilidades. Las funciones a su cargo son:

- Coordinar a las diferentes áreas del Banco en la implementación de planes y estrategias de continuidad.
- Coordinar la implementación de los planes de continuidad definidos, bajo la óptica de análisis de riesgos, análisis de impacto al negocio y estrategias de continuidad para asegurar que éstos atiendan las necesidades del negocio.
- Elaborar propuestas respecto a prioridades de procesos para la recuperación del negocio ante eventos de interrupción o desastre.
- Propender por el uso, entendimiento y divulgación de la estructura metodológica, políticas, roles, responsabilidades y definiciones del SGCN.
- Evaluar la respuesta ante la crisis o incidente e identificar oportunidades de mejora sobre el estado de preparación en continuidad del negocio del Banco.
- Presentar al Comité de Continuidad de Negocio, la gestión relacionada con el Plan de Recuperación de Procesos y los cambios a implementarse.
- Elaborar los reportes periódicos mencionados en este documento o los que a través de instrucciones se soliciten.
- Definir y gestionar los programas de capacitación sobre el plan de recuperación de procesos – BCP.
- Enviar a Grupo Aval los informes solicitados mediante instrucciones.
- Evaluar mínimo anualmente, a través del modelo de madurez corporativo, el SGCN.
- Asegurar el acompañamiento de personal especializado y que se considere necesario, durante las visitas que se realicen de parte de Grupo Aval y que estén relacionadas con la continuidad de negocio.
- Participar en las sesiones programadas por Grupo Aval del Comité Corporativo de Continuidad de Negocio.

- Validar la aplicación de los riesgos identificados en el catálogo de riesgos genérico de Grupo Aval.
- Coordinar pruebas para validar la eficacia de las medidas, acciones, políticas implementadas.
- Establecer controles operativos que aseguren y verifiquen la consistencia de la información enviada a Grupo Aval, con el fin de detectar posibles errores, de forma que se garantice que la información es consistente y veraz con la realidad de la entidad.
- Compartir las buenas prácticas utilizadas en el mercado.
- Ser el canal táctico de seguimiento, monitoreo y control del Conglomerado en las entidades.
- Cumplir con los lineamientos metodológicos contenidos en esta política.
- Definir planes de acción y realizar seguimiento a desviaciones presentadas en el plan de recuperación de procesos BCP.

6.10 VICEPRESIDENCIA DE TECNOLOGÍA

- Promover la efectividad y vigencia del sistema de gestión de continuidad de negocio.
- Mantener el patrocinio al sistema de gestión de continuidad de negocio.
- Participar en las reuniones de los diferentes comités de Alta Gerencia, cuando sea requerido por temas relacionados con Tecnología.
- Participar en el Comité de Continuidad de Negocio del Banco.
- Analizar el impacto que pudiese generar la situación o evento de crisis relacionados con la tecnología.
- Participar en el Comité de Administración de Crisis e informar los eventos generadores de la crisis.
- Dar lineamientos sobre la estructuración del Plan de Recuperación de Desastres.
- Liderar el análisis e impactos y la recolección información referente a la situación o evento de crisis asociados con tecnología, fuentes internas o externas involucradas.

6.11 GERENCIA TI DE OPERACIONES Y SERVICIOS DE TECNOLOGIA

- Gestionar la incorporación de los conceptos de continuidad en el diseño e implementación de los procesos y servicios de tecnología.
- Gestionar el presupuesto para el Plan de recuperación de desastres – DRP.
- Apoyar la puesta en marcha de las oportunidades de mejoramiento resultantes de la identificación y evaluación de riesgos y controles, así como las actividades administrativas de continuidad para mantener actualizados los planes de recuperación de tecnología.
- Realizar seguimiento a la definición de planes de acción en los eventos de indisponibilidad de alto impacto y/o relevantes relacionados con tecnología.
- Realizar seguimiento a la definición de planes de acción resultado de las evaluaciones efectuadas por la Tercera Línea de Defensa.
- Comunicar al Gerente de Ciberseguridad, Seguridad de la Información, Privacidad y Continuidad o al Director de Continuidad de Negocio los cambios en los procesos

relacionados con la tecnología del Banco que puedan afectar la efectividad de los planes de continuidad.
- Liderar las pruebas relacionadas con el plan de recuperación de desastres.
- Apoyar la implementación de los controles definidos para mitigar el riesgo de continuidad asociado a la concentración o pérdida del conocimiento.

6.12 DIRECTOR DE CONFIABILIDAD OPERATIVA DE TECNOLOGÍA Y DRP – PLAN DE RECUPERACIÓN DE DESASTRES

- El Director de Confiabilidad Operativa de TI y DRP, de la Gerencia TI de Operaciones y Servicios de Tecnología, es el responsable de coordinar la definición, implementación, pruebas y actualizaciones sobre el estado de preparación ante desastres e interrupciones de la plataforma tecnológica. Las funciones a su cargo son:
- Participar en el Comité de Continuidad de Negocio.
- Gestionar la actualización y probar el plan de recuperación ante desastres en los casos que se presenten situaciones como: modificaciones en la plataforma tecnológica, cambio en la estructura, roles y responsabilidades, cambios en los servicios tecnológicos, entre otros.
- Aportar el conocimiento de los diferentes planes y estrategias de continuidad de tecnología para que el Comité de Administración de Crisis tome decisiones.
- Coordinar pruebas relacionadas con el Plan de Recuperación de Desastres – DRP para validar la eficacia de las medidas, acciones, políticas implementadas.
- Apoyar la operación bajo contingencia y el retorno a la normalidad, del Plan de Recuperación ante Desastres.
- Presentar al Comité de Continuidad de Negocio, la gestión relacionada con el Plan de Recuperación de Desastres - DRP y los cambios a implementarse.
- Liderar el desarrollo, implementación y actualización de las estrategias y planes de recuperación ante desastres.
- Cumplir con los lineamientos metodológicos contenidos en esta política.
- Definir planes de acción y realizar seguimiento a desviaciones presentadas en el plan de recuperación de desastres - DRP
- Participar en las sesiones programadas por Grupo Aval del Comité Corporativo de Continuidad de Negocio.
- Evaluar la respuesta ante la crisis o incidente relacionados con tecnología e identificar oportunidades de mejora sobre el estado de preparación del plan de recuperación de desastres.
- Desarrollar e implementar los planes de acción resultado de las evaluaciones efectuadas por la Tercera Línea de Defensa.

6.13 GERENCIA DE EXPERIENCIA, MARCA Y SOSTENIBILIDAD

- Liderar el plan de comunicación de crisis y proponer los comunicados con la aprobación del Comité de Administración de Crisis.

- Participar en el Comité de Continuidad de Negocio, cuando sea convocado.
- Participar en las reuniones de los diferentes comités de Alta Gerencia, cuando sea requerido por temas relacionados con Comunicación de Crisis.
- Coordinar y dirigir las acciones de comunicación de crisis.
- Analizar el impacto que pudiese generar la situación o evento de crisis.
- Mantener contacto permanente con el Comité de Administración de Crisis y sus integrantes.
- Mantener contacto permanente con el o los Voceros Oficiales.
- Participar en las reuniones del Comité de Administración de Crisis e informar los eventos generadores de la crisis.
- Liderar el análisis e impactos y la recolección información referente a la situación o evento de crisis con las fuentes internas o externas involucradas.
- Realizar seguimiento a la definición de planes de acción resultado de las evaluaciones efectuadas por la Tercera Línea de Defensa.

6.14 GERENCIA DE COMUNICACIONES

- Participar en las reuniones de los diferentes comités de Alta Gerencia, cuando sea requerido por temas relacionados con Comunicación de Crisis.
- Difundir el Plan de Comunicación de Crisis en el Banco.
- Gestionar el presupuesto para el Plan de Comunicación de Crisis.
- Implementar las acciones de comunicación de crisis.
- Analizar el impacto que pudiese generar la situación o evento de crisis.
- Coordinar la logística necesaria para la emisión de los comunicados oficiales.
- Monitorear la información relacionada con la crisis.
- Participar en las pruebas y capacitaciones sobre el Sistema de Gestión de Continuidad de Negocio.
- Desarrollar e implementar los planes de acción resultado de las evaluaciones efectuadas por la Tercera Línea de Defensa.
- Presentar al Comité de Continuidad de Negocio, la gestión relacionada con el Plan de Comunicación de Crisis.
- Definir y gestionar los programas de capacitación relacionados con el Plan de Comunicación de Crisis.
- Definir planes de acción y realizar seguimiento a desviaciones presentadas en el Plan de Comunicación de Crisis

6.15 GERENCIA DE GESTIÓN Y DESARROLLO DEL TALENTO HUMANO

- Propender por la implementación efectiva de los controles que mitiguen los riesgos de no disponibilidad del recurso humano, que afectan la operación de los procesos críticos de negocio.
- Participar en el Comité de Continuidad de Negocio, cuando sea convocado.

- Informar al Director de Continuidad de Negocio sobre las novedades de colaboradores (ingresos, retiros, cambios de cargo, etc.) que hacen parte de los equipos de continuidad.
- Apoyar los procesos de capacitación sobre continuidad según lo coordinado con el Gerente de Ciberseguridad, Seguridad de la Información, Privacidad y Continuidad y Director de Continuidad de Negocio.
- Apoyar a las áreas en la implementación de prácticas de entrenamiento cruzado y transferencia de conocimiento, para el personal crítico de los procesos críticos del negocio.
- Gestionar el presupuesto para la formación del Talento Humano que conforma el Sistema de Gestión de Continuidad Negocio.
- Realizar seguimiento a la definición de planes de acción en los eventos de indisponibilidad de alto impacto y/o relevantes relacionados con el Talento Humano.
- Realizar seguimiento a la definición de planes de acción resultado de las evaluaciones efectuadas por la Tercera Línea de Defensa.

6.16 GERENCIA DE ATENCIÓN Y SERVICIO AL TALENTO HUMANO

- Participar en el Comité de Continuidad de Negocio, cuando sea convocado.
- Propender por la implementación de los controles que mitigan el riesgo de continuidad asociados a la no disponibilidad del recurso humano, propagación de epidemias o pandemias, atención o respuesta inadecuada a emergencias.
- Gestionar la identificación y actualización de los escenarios de riesgos que se puedan presentar en las instalaciones donde laboren colaboradores del Banco.
- Gestionar la contratación de personal en caso de que no se cuente con el personal requerido para la recuperación de procesos o la atención de una crisis.
- Gestionar el presupuesto para el Plan de Atención de Emergencias
- Realizar seguimiento a la definición de planes de acción en los eventos de indisponibilidad de alto impacto y/o relevantes relacionados con el Plan de Emergencias.
- Realizar seguimiento a la definición de planes de acción resultado de las evaluaciones efectuadas por la Tercera Línea de Defensa.

6.17 DIRECCIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO, DE LA GERENCIA DE ATENCIÓN Y SERVICIOS AL TALENTO HUMANO

- Participar en el Comité de Continuidad de Negocio, cuando sea convocado.
- Presentar al Comité de Continuidad de Negocio, la gestión relacionada con el Plan de Emergencia y los cambios a implementarse.
- Identificar y apoyar la implementación de los controles definidos para mitigar el riesgo de continuidad asociados a la no disponibilidad de recurso humano, propagación de epidemias o pandemias, atención o respuesta inadecuada a emergencias.
- Apoyar en el Comité de Administración de Crisis en las actividades de protección de la vida de los colaboradores durante la ocurrencia de un evento de crisis, con el apoyo del Equipo de Emergencias.

- Mantener la información sobre la situación de cualquier empleado que esté recibiendo servicios médicos o de otra índole a causa del desastre.
- Evaluar y actualizar los escenarios de riesgo que se puedan presentar en las instalaciones donde laboren colaboradores del Banco, con el apoyo del Director de Infraestructura.
- Asegurar la construcción, pruebas, capacitación y mantenimiento de los Planes de Emergencias en las instalaciones donde opera el Banco, tanto a nivel local como nacional.
- Definir y gestionar los programas de capacitación relacionados con el Plan de Emergencias.
- Definir planes de acción y realizar seguimiento a desviaciones presentadas en el Plan de Emergencias.
- Desarrollar e implementar los planes de acción resultado de las evaluaciones efectuadas por la Tercera Línea de Defensa.

6.18 GERENCIA DE ABASTECIMIENTO ESTRATÉGICO

- Gestionar la adquisición de bienes y suministros y contratación de servicios requeridos por los planes que conforman el Sistema de Gestión de Continuidad de Negocio.
- Gestionar todas las actividades de aseguramiento de activos, diferente a infraestructura física.
- Apoyar la implementación efectiva de los controles que mitiguen los riesgos de Continuidad asociados a los proveedores críticos relacionados con Continuidad de Negocio.
- Coordinar, con el apoyo de las aseguradoras, el acceso y revisiones para hacer efectivas las pólizas de seguros ante la materialización de eventos relacionados con el Sistema de Gestión de Continuidad de Negocio.

6.19 DIRECTOR DE INFRAESTRUCTURA – VICEPRESIDENCIA DE EXPERIENCIA DEL TALENTO HUMANO

- Participar en el Comité de Continuidad de Negocio, cuando sea convocado.
- Gestionar todas las actividades de aseguramiento de activos físicos del Banco.
- Realizar seguimiento permanente a los administradores de los edificios para asegurar la adecuada implementación de los controles definidos para la mitigación de los riesgos de continuidad asociados a las instalaciones físicas como son: La destrucción total o parcial de las instalaciones, inadecuada atención y prevención de incendios, no disponibilidad de servicios públicos.
- Mantener informado al Gerente de Ciberseguridad, Seguridad de la Información, Privacidad y Continuidad y Director de Continuidad de Negocio, con respecto a cambios efectuados en las instalaciones del Banco, así como traslados de personal de una instalación a otra, con el fin de evaluar el impacto que tendrán dichos cambios en los planes de recuperación de los procesos críticos.

- Apoyar la consecución e implementación de las adecuaciones físicas que se requieran en el Centro de Operación de Contingencia – COC o cualquier otra sede del Banco para retornar a la operación normal.

6.20 DIRECTOR DE SEGURIDAD BANCARIA

- Realizar el monitoreo permanente de las instalaciones del Banco a nivel nacional e informar al Gerente Oficial Corporativo de Riesgos sobre eventos relacionados con el Sistema de Gestión de Continuidad de Negocio.

- Realizar seguimiento permanente del ingreso a las instalaciones para evitar ingreso de personal no autorizado, imposibilidad de acceso a las instalaciones, robo o pérdida de activos, atención o respuesta inadecuada a emergencias, e inadecuado mantenimiento de la infraestructura física.

6.21 GERENCIA DE CONTROLORÍA

- Evaluar el cumplimiento de las políticas y de los planes que conforman el Sistema de Gestión de Continuidad de Negocio del Banco.
- Adelantar las pruebas de auditoría que considere apropiadas de acuerdo con el plan de trabajo anual aprobado por el Comité de Auditoría del Banco
- Generar los informes de las evaluaciones realizadas al cumplimiento de la política y de los planes que conforman el Sistema de Gestión de Continuidad de Negocio del Banco.

6.22 GERENTE DUEÑO DE PROCESO

Antes del desastre o interrupción

- Mantener vigente y efectivo el plan de recuperación de los procesos críticos.
- Propender por la correcta operación de los procesos críticos de negocio tanto en operación normal como durante una crisis.
- Gestionar los recursos requeridos para definir, actualizar, divulgar, custodiar y ejecutar los planes de recuperación de sus procesos críticos.
- Gestionar los recursos requeridos para el Centro de Operación en Contingencia (si se requiere).
- Velar porque los proveedores críticos de su(s) proceso(s) críticos de negocio estén preparados para prestar sus servicios inclusive ante eventos de crisis.
- Asegurar la definición e implementación de mecanismos para garantizar el desplazamiento desde y hacia los centros de comando y centros alternos de operación.
- Participar en el Comité de Continuidad de Negocio cuando sea convocado.
- Coordinar con los Directores de Continuidad de Negocio y Confiabilidad Operativa de Tecnología – DRP, la ejecución, actualización y pruebas de los planes de recuperación para los procesos críticos a su cargo.

- Coordinar, en conjunto con el Director de Continuidad de Negocio, las necesidades de ajuste de las estrategias y Plan de Recuperación del Proceso.
- Informar a la Gerencia de Ciberseguridad, Seguridad de la Información, Privacidad y Continuidad y al Director de Continuidad de Negocio sobre cambios organizacionales que puedan afectar la efectividad de sus planes de recuperación de procesos y por ende generan necesidades de actualización o ajuste, como:

    - Novedades de colaboradores (ingresos, retiros, cambios de cargo, etc.) que hacen parte de los equipos de continuidad.
    - Cambios en el modelo operativo de los procesos
    - Cambios en los recursos (tecnología, infraestructura, proveedores, entre otros) que soportan los procesos.

- Coordinar las pruebas del plan de recuperación de procesos.
- Asegurar la ejecución de los programas de pruebas de acuerdo con lo mínimo requerido por el Director de Continuidad de Negocio o cuando se presenten cambios relevantes en sus procesos críticos, sobre los planes de recuperación, la disponibilidad y actualización oportuna de los registros vitales, recursos y colaboradores requeridos para que su proceso opere ante un evento de crisis.
- Documentar el resultado de las pruebas efectuadas.

Durante el desastre o interrupción

- Liderar los procedimientos de recuperación de los procesos críticos de negocio a su cargo durante una crisis.
- Coordinar las actividades administrativas requeridas para mantener actualizados los procedimientos de recuperación y retorno a operación normal del proceso.
- Participar en el Comité de Administración de Crisis si se requiere, según la magnitud y extensión de los daños.
- Liderar las actividades del equipo de recuperación.
- Comunicar al Gerente de Ciberseguridad, Seguridad de la Información, Privacidad y Continuidad y al Director de Continuidad de Negocio el estado de la recuperación de su(s) proceso(s) de negocio.
- Liderar las operaciones de retorno a operación normal.
- Generar reportes específicos sobre la ejecución de los procedimientos de recuperación, durante y después de la crisis.
- Comunicar al Comité de Administración de Crisis las causas y detalles del incidente que conllevó a la operación en contingencia.

Después del desastre o interrupción

- Identificar las necesidades de ajuste a planes y estrategias según las lecciones aprendidas como consecuencia del desastre e interrupción.

CONTROL DE CAMBIOS

HISTORIAL		
# VERSIÓN	**FECHA PUBLICACIÓN**	**DESCRIPCIÓN DEL CAMBIO**
1	14/08/2018	• Se actualiza la política del subproceso “Sistema Gestión Continuidad del Negocio” realizando una revisión completa de codificación de anexos y formas electrónicas relacionadas. • Se incluye dentro de los miembros del comité de Continuidad del Negocio a la Gerencia Experiencia de Marca y Gerencia de Gestión y Desarrollo del Talento Humano. • Se incluye dentro de los miembros del Gobierno de Continuidad del Negocio a la Vicepresidencia de Tecnología y Productividad y Gerencia Experiencia de Marca. • Se actualizan los roles y responsabilidades de la Dirección de Continuidad de Negocio eliminando “Monitorear la evolución del riesgo de no disponibilidad de los procesos de negocio”.
2	25/02/2021	Se reestructura el documento de política acorde con lineamiento de política corporativa AVAL, la cual tiene como objetivo establecer los lineamientos generales para la adecuada implementación y mantenimiento del SGCN en Grupo Aval y sus Entidades Subordinadas.
3	6/05/2024	Se modifica el cargo Gerente Integral de Riesgos por Vicepresidente de Riesgos Se actualizan los cargos con relación a los cambios en la Estructura General del Banco.