



## RESOLUCIÓN ADMINISTRATIVA NRO. BCE-GG-010-2025

### GERENTE GENERAL

### BANCO CENTRAL DEL ECUADOR

#### CONSIDERANDO:

- Que,** la Constitución de la República del Ecuador, en su artículo 226, prescribe que las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la Ley;
- Que,** el artículo 227 ibidem señala que la Administración Pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, entre otros;
- Que,** el inciso primero del artículo 303 ut supra establece que el Banco Central del Ecuador es una persona jurídica de derecho público, cuya organización y funcionamiento será establecido por la Ley; y que instrumentará la política monetaria, crediticia, cambiaria y financiera que expida la Función Ejecutiva;
- Que,** el artículo 26 del Código Orgánico Monetario y Financiero determina que el Banco Central del Ecuador es una persona jurídica de derecho público, parte de la Función Ejecutiva, de duración indefinida, con autonomía institucional, administrativa, presupuestaria y técnica; que en el ejercicio de sus funciones y atribuciones se regirá por la Constitución de la República, el Código Orgánico Monetario y Financiero, su estatuto, las regulaciones expedidas por el órgano de gobierno, los reglamentos internos y las demás leyes aplicables en razón de la materia;
- Que,** los numerales 1 y 2 del artículo 49 ut supra, como funciones del Gerente General del Banco Central del Ecuador, establecen: “1. *Ejercer la representación legal, judicial y extrajudicial del Banco Central del Ecuador para todos los efectos;*  
2. *Dirigir y coordinar el funcionamiento del Banco Central del Ecuador en sus aspectos, técnico, administrativo, operativo y de personal, para lo cual expedirá los reglamentos internos correspondientes; y, de lo cual responde ante la Junta de Política y Regulación Monetaria (...)*”;
- Que,** el artículo 128 del Código Orgánico Administrativo, sobre los actos normativos de carácter administrativo, determina: “*Es toda declaración unilateral efectuada en ejercicio de una competencia administrativa que produce efectos jurídicos generales, que no se agota con su cumplimiento y de forma directa*”;



**Que,** el artículo 130 ibidem dispone: *“Las máximas autoridades administrativas tienen competencia normativa de carácter administrativo únicamente para regular los asuntos internos del órgano a su cargo, salvo los casos en los que la ley prevea esta competencia para la máxima autoridad legislativa de una administración pública.*

*La competencia regulatoria de las actuaciones de las personas debe estar expresamente atribuida en la ley”;*

**Que,** mediante Resolución Nro. JPRM-2022-007-M, de 23 de febrero de 2022, se expidió la “Política para la Administración Integral de Riesgos del Banco Central del Ecuador”;

**Que,** la Junta de Política y Regulación Monetaria, mediante Resolución Nro. JPRM-2023-011-G, de 30 de mayo de 2023, expidió el “Reglamento de conformación y funcionamiento de los Comités Institucionales del Banco Central del Ecuador”, el cual fue reformado mediante Resoluciones Nro. JPRM-2023-017-G, de 28 de septiembre de 2023; y, Nro. JPRM-2024-009-G, de 15 de mayo de 2024;

**Que,** la letra e) del artículo 26 de la referida Resolución, como una de las funciones del Comité de Administración Integral de Riesgos, establece: *“Conocer los resultados de las pruebas periódicas de contingencia y continuidad del negocio, así como el avance de la implementación de las recomendaciones efectuadas y acciones de mejora”;*

**Que,** mediante Resolución Nro. JPRM-2024-005-A, de 8 de marzo de 2024, la Junta de Política y Regulación Monetaria emitió el *“Estatuto Orgánico de Gestión Organizacional por Procesos del Banco Central del Ecuador”*, que establece la estructura, competencias, planificación y modelo de gestión del Banco Central del Ecuador;

**Que,** la letra e) del artículo 4 de la Resolución Administrativa Nro. BCE-GG-024-2023, de 29 de noviembre de 2023, reformada mediante Resolución Administrativa Nro. BCE-GG-012-2024, señala que el Comité de Administración Integral de Riesgos debe: *“Conocer los resultados semestrales de las pruebas de entrenamiento y anuales de las pruebas de contingencia y continuidad de negocio; así como, el avance de la implementación de las recomendaciones efectuadas y acciones de mejora, mediante informes presentados por la Subgerencia de Riesgos de Operaciones”;*

**Que,** mediante Acuerdo Nro. 004-CG-2023, de 7 de febrero de 2023, la Contraloría General del Estado expidió las *“Normas de control interno para las entidades, organismos del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos”;*



**Que,** mediante Informe Técnico Nro. BCE-GR-2025-042 / BCE-SRO-2025-008, de 12 de junio de 2025, la Gerencia de Riesgos y la Subgerencia de Riesgos de Operaciones emitieron su criterio técnico favorable y recomendaron la suscripción de la presente resolución;

**Que,** mediante Informe Jurídico Nro. BCE-GJ-025-2025, de 23 de junio de 2025, el Gerente Jurídico establece la pertinencia de que el señor Gerente General del Banco Central del Ecuador suscriba y expida el acto normativo correspondiente, sin que exista impedimento legal para la emisión del mismo y recomienda que el proyecto de Resolución Administrativa, sea puesto en su conocimiento;

**Que,** mediante Resolución Nro. JPRM-2022-022-A, de 19 de septiembre de 2022, la Junta de Política y Regulación Monetaria designó al magíster Guillermo Enrique Avellán Solines, como Gerente General del Banco Central del Ecuador; y,

En ejercicio de sus funciones y atribuciones, resuelve expedir el:

## **PLAN DE ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS OPERACIONES DEL BANCO CENTRAL DEL ECUADOR**

### **CAPÍTULO I LINEAMIENTOS GENERALES DEL PLAN DE CONTINUIDAD**

**Artículo 1.- Plan de Continuidad:** El Banco Central del Ecuador implementará el Plan de Continuidad como componente esencial de la administración integral de riesgos, con la finalidad de garantizar la capacidad para ejecutar sus procesos, productos o servicios críticos, en caso de registrarse una interrupción, independientemente de su origen o naturaleza.

**Artículo 2.- Objetivos:** El Plan de Continuidad tiene los siguientes objetivos:

- a) Minimizar la probabilidad de interrupciones en las operaciones de los procesos, productos o servicios críticos, identificados a través de la metodología de análisis de impacto del negocio;
- b) Asegurar una rápida y efectiva restauración de las operaciones afectadas por incidentes; y,
- c) Capacitar al personal para enfrentar posibles incidentes, que permita asegurar la protección de la integridad de las personas y bienes en forma adecuada.

**Artículo 3.- Definiciones:** Para efecto de la presente norma, se aplicarán las siguientes definiciones:



- a) **Actividad:** Conjunto de una o más tareas que tienen una salida definida.
- b) **Análisis de impacto de negocio:** Proceso para evaluar el impacto que una interrupción en las operaciones críticas tendría en la Institución, considerando los tiempos y recursos necesarios para la recuperación.
- c) **Causa de interrupción por ausencia de personal:** Se presenta cuando el o los responsables de ejecutar procesos críticos no pueden asistir a su puesto de trabajo para desarrollar las actividades correspondientes de su cargo.
- d) **Causa de interrupción por causas tecnológicas:** Se presenta cuando uno o varios componentes de los sistemas de información (hardware o software) experimentan fallas o interrupciones prolongadas, incluyendo ciberataques, fallas en telecomunicaciones (Internet, redes privadas o sistemas de comunicación) o errores humanos.
- e) **Causa de interrupción por no disponibilidad del sitio normal de trabajo:** Ocurre por un evento fortuito o de fuerza mayor (como desastre natural, emergencia sanitaria, actividad terrorista, problemas de transporte, huelgas, entre otros), que impide al personal acceder a su lugar de trabajo para desarrollar las actividades.
- f) **Centro de datos:** Instalación física que alberga la infraestructura tecnológica utilizada para crear, ejecutar y entregar aplicaciones y servicios. Además, almacena y gestiona los datos asociados con esas aplicaciones y servicios.
- g) **Impacto:** Resultado de un incidente que afecta la capacidad de la Institución para operar y cumplir sus objetivos.
- h) **Incidente:** Evento imprevisto que puede causar o llevar a una interrupción, reducción o alteración de las operaciones normales de la Institución.
- i) **Interrupción:** Incidente, ya sea anticipado o no, que provoca una desviación no planificada y negativa en la entrega esperada de productos y servicios, en relación con los objetivos de una organización.
- j) **Objetivo:** Resultado deseado o meta a alcanzar.
- k) **Parte interesada (stakeholder):** Persona u organización que puede influir, verse afectada o percibirse afectada por una decisión o actividad.
- l) **Proceso:** Conjunto de actividades interrelacionadas o interactivas que transforman entradas en salidas.



- m) **Procesos, productos o servicios críticos:** Conjunto de actividades esenciales para la continuidad del negocio y las operaciones de la Institución, cuya falta de identificación o aplicación deficiente podrían generar impactos negativos en los ámbitos financiero, reputacional y legal.
- n) **Producto y servicio:** Resultado o salida proporcionada por una organización a las partes interesadas.
- o) **Punto de recuperación objetivo (RPO):** Cantidad máxima aceptable de pérdida de datos (en minutos u horas) que un área puede tolerar sin afectar gravemente las operaciones. Este tiempo debe ser acordado entre el Gerente de cada área (responsable del activo de información) y la Gerencia de Tecnologías de la Información. Se mide desde la copia de seguridad más reciente hasta la interrupción del servicio de TIC.
- p) **Recuperación tecnológica:** Proceso de restauración o recuperación de sistemas, datos o infraestructura tecnológica que han fallado, han sido dañados o se han perdido, con el fin de restablecer su funcionamiento normal y reanudar las operaciones en el menor tiempo posible. Incluye la reparación de equipos, la recuperación de información y la restauración de servicios tecnológicos.
- q) **Riesgo:** Posibilidad de que un evento ocurra y genere pérdidas financieras para la Institución.
- r) **Riesgos tecnológicos:** Posibles eventos o situaciones adversas derivados del uso de tecnologías que pueden afectar negativamente a una organización, sus operaciones o sus datos. Estos riesgos incluyen fallos en sistemas, ciberataques, obsolescencia tecnológica, pérdida de datos, problemas de seguridad y privacidad, entre otros.
- s) **Tecnología de la información y comunicación (TIC):** Conjunto de herramientas y métodos utilizados para administrar la información. Incluye hardware, software, sistemas operativos, sistemas de gestión de bases de datos, redes, multimedia, servicios asociados, entre otros.
- t) **Tiempo de recuperación de trabajo (WTR):** Máximo tiempo tolerable para que el área operativa verifique la integridad de los datos. Esto incluye tareas como verificar y/o configurar las bases de datos, verificar registros y asegurar que las aplicaciones estén funcionando correctamente y sean accesibles. Este tiempo es un segmento del MTPD y debe ser definido por el Gerente de cada área (responsable del activo de información). Se mide desde la finalización de la fase de recuperación del servicio hasta el reinicio de las operaciones.



- u) **Tiempo de Recuperación Objetivo (RTO):** Tiempo disponible para que la Gerencia de Tecnologías de la Información recupere los sistemas y recursos interrumpidos. Este tiempo es un segmento del MTPD e incluye actividades como: identificación del evento de interrupción, análisis inicial, notificación a la comisión de continuidad, acciones de recuperación de servicio en el sitio principal, acciones de recuperación en el sitio alterno. Este tiempo se determina como la diferencia entre el MTPD y el WRT. Se mide desde la interrupción del servicio de TIC hasta el fin de fase de recuperación del servicio.
- v) **Tiempo Máximo de Inactividad Tolerable (MTPD):** Periodo máximo que un proceso de negocio puede tolerar la ausencia o indisponibilidad de un servicio crítico. Este tiempo debe ser definido por el Gerente de cada área (responsable del activo de información), basado en su conocimiento del negocio, eventos previos y pruebas de continuidad realizadas anteriormente. Se mide desde la interrupción del servicio de TIC hasta el reinicio de operaciones.

**Artículo 4.- Alcance:** El Plan de Continuidad aplica para todas las áreas del Banco Central del Ecuador que tengan procesos, productos o servicios críticos, identificados a través de la metodología de análisis de impacto del negocio, con el fin de que la Institución esté preparada para continuar sus operaciones luego de producido un incidente. Esta metodología la definirá y aplicará la Subgerencia de Riesgos de Operaciones.

**Artículo 5.- Componentes:** El Plan de Continuidad se compone de:

- a) Planes de Contingencia de las áreas con procesos, productos o servicios críticos;
- b) Planes de Contingencia de Tecnología de la Información;
- c) Planes de Emergencia y Evacuación;
- d) Planes de Comunicación de Gestión de Crisis; y,
- e) Plan de Respuesta ante Incidentes.

**Artículo 6.- Pruebas de entrenamiento periódicas de contingencia:** Las áreas que gestionan procesos, productos o servicios críticos llevarán a cabo pruebas de entrenamiento de sus planes de contingencia, con el objetivo de verificar la disponibilidad de los servicios necesarios para asegurar su operatividad.

Las pruebas evaluarán la disposición y preparación del personal alterno involucrado en la continuidad de las operaciones frente a un incidente. La Subgerencia de Riesgos de Operaciones dará seguimiento a la ejecución de las pruebas del plan de contingencia, a fin de verificar la disponibilidad de los servicios y equipos informáticos necesarios, así como del entrenamiento planificado por las áreas que mantienen procesos, productos o servicios críticos, de conformidad con el cronograma que será solicitado por la Subgerencia de Riesgos de Operaciones al inicio de cada año.



**Artículo 7.- Prueba global de contingencia:** El Banco Central del Ecuador, con el fin de evaluar la efectividad de las estrategias de recuperación de las operaciones definidas en los planes de contingencia de las áreas con procesos, productos o servicios críticos, así como los planes de contingencia de tecnologías de la información, ejecutará al menos, una vez al año, una prueba global de contingencia de dichos planes.

La Subgerencia de Riesgos de Operaciones coordinará la ejecución de las pruebas de contingencia y comunicará los resultados a las autoridades del Banco.

## **CAPÍTULO II**

### **DE LA ESTRUCTURA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**

**Artículo 8.- Comisión de Continuidad:** La Comisión de Continuidad estará integrada por el Subgerente General, que cumplirá el rol de Líder de la Comisión; y, el Gerente de Riesgos, que cumplirá el rol de Director de Continuidad.

En caso de que se presenten interrupciones por caídas en los sistemas tecnológicos y de información o no disponibilidad del sitio normal de trabajo, la Comisión será la responsable de evaluar dichas interrupciones en los diferentes procesos, productos y servicios críticos, así como los tiempos de recuperación objetivo y, si es necesario, activará los planes de contingencia del negocio o dará inicio y fin, al plan de contingencia.

La Comisión informará inmediatamente a las Gerencias que mantienen procesos, productos y servicios críticos, sobre las decisiones tomadas e informará a la Gerencia General, por escrito, dentro del plazo de un (1) día, sobre las decisiones tomadas dentro del plan de contingencia.

**Artículo 9.- Líder de Continuidad:** El Subgerente de Riesgos de Operaciones cumplirá el rol de Líder de Continuidad, encargado de gestionar el plan de continuidad. El Líder de Continuidad tendrá las siguientes responsabilidades:

- a) Coordinar con las áreas que mantienen procesos, productos o servicios críticos, la evaluación de riesgos y actualización de los planes de contingencia de la Institución, facilitando el acompañamiento metodológico;
- b) Elaborar y mantener actualizado el Plan de Respuesta ante incidentes, en coordinación con los Coordinadores de Recuperación;
- c) Identificar los nuevos riesgos que afecten la continuidad de la operación normal de la Institución, evidenciando las posibles debilidades del plan de continuidad;
- d) Coordinar, con los Coordinadores de Recuperación, la ejecución de las pruebas del plan de continuidad de las áreas que mantienen procesos, productos y servicios críticos;
- e) Monitorear el estado de recuperación de la entidad durante una contingencia y comunicar a la Comisión de Continuidad;





- f) Coordinar, con las áreas que manejan procesos, productos o servicios críticos, el análisis de las causas que provocaron el evento de contingencia;
- g) Promover, conjuntamente con las unidades administrativas que manejan procesos, productos o servicios críticos, la mejora continua de los planes de contingencia, a través de la definición de estrategias que reduzcan el impacto y la probabilidad de ocurrencia;
- h) Promover la actualización de los planes de emergencia y evacuación de la institución, y asegurar su difusión entre todos los funcionarios del Banco, con el objetivo de garantizar el bienestar del personal y minimizar los riesgos en caso de una emergencia;
- e,
- i) Informar al Comité de Administración Integral de Riesgos y Gerencia General los resultados de las pruebas periódicas, parciales y prueba global de contingencia, así como el avance de la implementación de las recomendaciones efectuadas y acciones de mejora.

**Artículo 10.- Coordinadores de Recuperación:** El Gerente de Medios de Pagos y Servicios Nacionales, el Gerente de Inversiones y Servicios Internacionales; y, el Subgerente Financiero son Coordinadores de Recuperación, quienes serán responsables de liderar la recuperación de sus procesos, productos o servicios críticos, de conformidad con las estrategias de contingencia definidas en el ámbito de sus competencias; y, de coordinar con el Líder de Recuperación Tecnológica y Director de Continuidad.

Los Coordinadores de Recuperación actúan como el enlace directo entre los procesos, productos y servicios críticos y el Director de Continuidad, además de proporcionar información a la Comisión de Continuidad sobre las decisiones tomadas antes, durante y después de la declaración de inicio y fin de la contingencia. Los Coordinadores de Recuperación tendrán las siguientes responsabilidades:

- a) Liderar las reuniones con los Administradores del Plan de Continuidad, para diagnosticar y evaluar los incidentes que están afectando la prestación del servicio, a fin de determinar el inicio del estado de contingencia del área; o, proveer de información a la Comisión de Continuidad para activar el Plan Global de Contingencia;
- b) Asesorar a la Comisión de Continuidad sobre la pertinencia del inicio del estado de contingencia;
- c) Instruir a los equipos de recuperación y al personal del sitio alternativo de datos, la ejecución de los planes de contingencia, ante el incidente ocurrido, y asegurar la continuidad de los procesos, productos o servicios críticos a los usuarios;
- d) Identificar posibles riesgos y debilidades que podrían afectar la continuidad de su operación normal y reportarlos a la Subgerencia de Riesgos de Operaciones, para su gestión;
- e) Informar a los proveedores y usuarios externos, en los casos que corresponda, sobre el estado de contingencia, previa decisión y autorización de la Comisión de Continuidad;





- f) Informar a la Comisión de Continuidad sobre el estado de la recuperación de sus procesos, productos o servicios críticos;
- g) Velar por la realización de las pruebas del Plan de Continuidad, revisar los resultados obtenidos y aplicar las opciones de mejora en caso de que corresponda;
- h) Verificar por mantener actualizado permanentemente los planes de contingencia relacionados a los procesos, productos o servicios críticos, en los casos que se presenten cambios en los aplicativos, procesos, roles y responsabilidades, disponibilidad de los recursos, entre otros; los mismos que deben ser remitidos a la Subgerencia de Riesgos de Operaciones; e,
- i) Asegurar la correcta ejecución de las pruebas de entrenamiento, en el sitio alternativo, de los procesos, productos o servicios críticos que realizan las áreas a cargo de los coordinadores de recuperación.

**Artículo 11.- Líder de Recuperación Tecnológica:** El Gerente de Tecnologías de la Información cumplirá el rol de Líder de Recuperación Tecnológica y será el encargado de la recuperación tecnológica de todos los procesos, productos o servicios críticos de Tecnologías de la Información (TI), siguiendo las estrategias definidas en los planes de contingencia. El Líder de Recuperación Tecnológica tendrá las siguientes responsabilidades:

- a) Notificar la interrupción de los servicios tecnológicos al Líder de Continuidad;
- b) Recomendar a la Comisión de Continuidad el inicio del estado de contingencia, en los casos de una interrupción originada en causas tecnológicas;
- c) Liderar la recuperación tecnológica, aplicando las estrategias de continuidad definidas en sus planes de contingencia;
- d) Identificar y gestionar los posibles riesgos tecnológicos que afectan a la continuidad de la operación normal de la Institución y que afecten a los procesos, productos y servicios críticos;
- e) Mantener comunicación permanente con los Coordinadores de Recuperación durante el estado de contingencia, desde la identificación del incidente;
- f) Coordinar la continuidad de los servicios tecnológicos proporcionados por los proveedores externos en el estado de contingencia;
- g) Informar sobre el estado de la recuperación de los servicios tecnológicos a la Comisión de Continuidad;
- h) Actualizar los planes de contingencia de tecnologías de la información, considerando cualquier cambio que pueda afectarlos, tales como modificaciones en los aplicativos, cambios en la infraestructura, en roles y responsabilidades, y variaciones en la disponibilidad de recursos, entre otros;
- i) Velar por la realización de las pruebas de entrenamiento del Plan de Contingencia de Tecnologías de la Información, evaluar los resultados obtenidos en las mismas y aplicar las opciones de mejora que corresponda; y,
- j) Asegurar la disponibilidad de la infraestructura tecnológica para la operación remota y en sitios alternos de operación.



**Artículo 12.- Líder Administrativo:** El Gerente Administrativo Financiero cumplirá el rol de Líder Administrativo y será el encargado de coordinar los aspectos logísticos internos en estado de contingencia. El Líder Administrativo tendrá las siguientes responsabilidades:

- a) Coordinar el abastecimiento de elementos esenciales como transporte, recursos humanos, de infraestructura y suministros;
- b) Coordinar la adecuación de los centros alternos de operaciones, en caso de que la situación lo amerite; y,
- c) Mantener informada a la Comisión de Continuidad sobre incidentes por falta de suministro de elementos esenciales.

**Artículo 13.- Administradores del Plan de Continuidad:** Son los Subgerentes, o quienes hagan sus veces, de cada una de las unidades administrativas que mantienen procesos críticos para la Continuidad. Los Administradores del Plan de Continuidad tendrán las siguientes responsabilidades:

- a) Definir el equipo de recuperación de su área, en función de sus procesos, productos o servicios críticos;
- b) Actuar como contraparte del área a la que representa para los asuntos relacionados a la continuidad del negocio con los Coordinadores de Recuperación;
- c) Cumplir con las actividades y fechas establecidas en el cronograma de plan de pruebas de entrenamiento;
- d) Mantener informados a todos los colaboradores de sus respectivas áreas acerca de los planes de contingencia que les corresponde;
- e) Asegurar la correcta aplicación de los planes de contingencia al interior del área;
- f) Mantener actualizados los documentos de los planes de contingencia del proceso al que representan y difundir de manera periódica al personal a su cargo;
- g) Analizar el impacto del incidente en un evento de interrupción; y, en el caso de aplicarse una contingencia, en donde se requiera activar el personal operativo de la ciudad de Guayaquil o Cuenca (sitio alternativo), deberá comunicar al Líder de Continuidad para la respectiva coordinación; y,
- h) Reportar cualquier incidente o evento de interrupción al Líder de Recuperación del área correspondiente y al Líder de Continuidad.

**Artículo 14.- Líder de Comunicación:** El Subgerente de Comunicación Estratégica cumplirá el rol de Líder de Comunicación y será el encargado de asesorar y coordinar con la Comisión de Continuidad, la comunicación, tanto a nivel interno (colaboradores) como a nivel externo (clientes, proveedores, alianzas, organismos de control, entre otros), ante eventos de interrupción, de acuerdo con el Plan de Comunicación de Gestión de Crisis.



**Artículo 15.- Líder de Emergencia:** El Subgerente de Operaciones de Seguridad y Transporte de Valores cumplirá el rol de Líder de Emergencia y será el encargado de coordinar los aspectos de emergencia y evacuación internos en estado de contingencia. El Líder de Emergencia tendrá las siguientes responsabilidades:

- a) Mantener actualizados los planes de emergencia y evacuación ante cualquier cambio que afecte a los mismos;
- b) Socializar al personal acciones preventivas, relacionadas a la aplicación de los planes de emergencia;
- c) Velar por la realización de las pruebas (simulacros) de los planes de emergencia y evacuación, evaluar los resultados obtenidos en las mismas y aplicar el plan de mitigación que corresponda; y,
- d) Establecer y ejecutar el programa de capacitaciones a los brigadistas; y, velar por la constante actualización de la base de brigadistas, en cada uno de los edificios del Banco Central del Ecuador.

### **CAPÍTULO III**

#### **DEL INICIO Y FINALIZACIÓN DEL ESTADO DE CONTINGENCIA OPERATIVA**

**Artículo 16.- Inicio del estado de contingencia operativo:** Ante cualquier interrupción que afecte procesos, productos o servicios críticos, los Coordinadores de Recuperación y/o el Líder de Recuperación Tecnológica deberán notificar de inmediato a la Comisión de Continuidad para que se considere el inicio del estado de contingencia operativo. La Comisión evaluará la situación y tomará las decisiones en función de las causas de la interrupción. Las causas de interrupción serán ausencia de personal, no disponibilidad del sitio de trabajo habitual; y, causas tecnológicas.

La Comisión de Continuidad declarará el inicio del estado de contingencia operativa mediante resolución administrativa suscrita por el Líder de la Comisión, que será comunicada al Gerente General y a todas las áreas operativas necesarias para superar el estado de contingencia.

**Artículo 17.- Ausencia de personal:** Cuando se presente ausencia de personal, los Coordinadores de Recuperación serán responsables de evaluar la situación e implementar una estrategia de capacitación cruzada que permita al personal asumir diversas funciones, minimizando el impacto de la ausencia de miembros clave del equipo; implementar el teletrabajo a través de herramientas digitales de colaboración y comunicación que permitan al personal seguir realizando sus tareas desde cualquier lugar; e, integrar sistemas automáticos que reduzcan la dependencia de las tareas manuales de manera que puedan ejecutarse sin intervención constante del personal. Además, ejecutarán los planes de acuerdo con las acciones definidas previamente en la estrategia de recuperación.



**Artículo 18.- No disponibilidad del sitio de trabajo habitual:** Frente a la no disponibilidad del sitio de trabajo habitual, la Comisión de Continuidad evaluará el riesgo e implementará la modalidad de teletrabajo, a partir de la alerta de los Coordinadores de Recuperación o Líder de Emergencia. Para ello, la Gerencia de Tecnologías de la Información debe garantizar el acceso y uso remoto de plataformas digitales de comunicación y gestión de documentos; y, contar con soluciones tecnológicas que permitan replicar datos y aplicaciones en el centro de datos, que permitan asegurar que los procesos, productos y servicios críticos puedan continuar sin interrupciones, manteniendo un adecuado esquema de control y seguridad.

**Artículo 19. - Causas tecnológicas:** Cuando se presenten fallos tecnológicos, los Coordinadores de Recuperación o el Líder de Recuperación Tecnológica notificarán a la Comisión de Continuidad y se procederá a evaluar los tiempos de recuperación objetivos (RTO) de los procesos, productos y servicios críticos.

Si el RTO es menor a tres (3) horas, se procederá a restaurar los productos y servicios críticos en el sitio principal del centro de datos. Caso contrario, se levantarán los procesos, productos y servicios críticos en el sitio alternativo del centro de datos y se informará al Gerente General sobre el avance y las acciones tomadas.

**Artículo 20. - Finalización del estado de contingencia operativo:** Los Coordinadores de Recuperación informarán a la Comisión de Continuidad las acciones realizadas ante la interrupción de procesos, productos o servicio críticos frente a los escenarios de ausencia de personal y no disponibilidad del sitio de trabajo habitual.

Ante el escenario de fallos tecnológicos, el Líder de Recuperación Tecnológica notificará a los Coordinadores de Recuperación y a la Comisión de Continuidad, la habilitación de los servicios y sistemas de los procesos críticos y el retorno a la normalidad; ante lo cual la Comisión dará por finalizado el estado de contingencia mediante resolución administrativa, suscrita por el líder de la Comisión, e informará al Gerente General.

**DISPOSICIÓN GENERAL ÚNICA:** El sitio principal del centro de datos será la ciudad de Quito; y, el sitio alternativo del centro de datos será la ciudad de Guayaquil.

**DISPOSICIÓN TRANSITORIA ÚNICA:** En el plazo de seis (6) meses, contados a partir de la suscripción de la presente resolución, la Gerencia de Riesgos, en coordinación con la Gerencia de Planificación y Gestión Estratégica, la Gerencia de Medios de Pago y Servicios Nacionales, la Gerencia de Inversiones y Servicios Internacionales y la Gerencia de Tecnologías de la Información, gestionarán la emisión o actualización de los documentos procedimentales internos pertinentes para la aplicación de la presente resolución.

**DISPOSICIÓN FINAL.-** La presente Resolución entrará en vigencia a partir de su publicación en el Registro Oficial.



Encárguese a la Secretaría General de la publicación de la presente Resolución en el Registro Oficial y en la página web institucional.

**COMUNÍQUESE Y PUBLÍQUESE.** – Dada en la ciudad de Quito, Distrito Metropolitano, a 25 de junio de 2025.

Mgs. Guillermo Avellán Solines  
**GERENTE GENERAL**  
**BANCO CENTRAL DEL ECUADOR**