

(...)

VIGÉSIMA QUINTA. - CLÁUSULA DE RESPONSABILIDADES EN GESTIÓN DE

RIESGOS: El **CONTRATISTA** implementará y mantendrá, durante toda la vigencia del contrato, un sistema o modelo de gestión de riesgos cuando resulte aplicable que sea adecuado y proporcional al alcance y criticidad de los servicios contratados y cuyo objetivo es el de identificar, administrar, controlar, mitigar y monitorear de manera adecuada y efectiva los riesgos; principalmente operacionales, de continuidad del negocio, de conductas y todos los riesgos asociados a la prestación de los servicios contratados que pueden afectar el cumplimiento del objeto contractual, los niveles de servicio pactados, la calidad, la continuidad de la operación y, cuando aplique, los derechos y la experiencia del consumidor financiero.

Lo anterior se realizará sin perjuicio de las obligaciones específicas en materia de seguridad de la información, ciberseguridad y protección de datos, de conformidad con lo establecido en el contrato y la normatividad vigente. Para su cumplimiento, el **CONTRATISTA** debe como mínimo, atender lo siguiente:

i) Identificación y controles: Gestionar los riesgos que se derivan de la prestación del servicio teniendo en cuenta lo siguiente:

- a) Identificar los riesgos y sus causas generadoras que se deriven del desarrollo de la prestación del servicio contratado;
- b) Implementar y documentar los controles que mitiguen las causas que generen la materialización de los riesgos;
- c) Realizar la medición de probabilidad e impacto de los riesgos identificados;
- d) Contar con los procedimientos necesarios para verificar el cumplimiento de las obligaciones establecidas en el contrato;
- e) Contar con políticas o lineamientos en gestión de riesgos;
- f) Realizar monitoreo periódico sobre la gestión de riesgos de la empresa.
- g) Permitir al **BANCO** la consulta y/o verificación de la información suministrada sobre el mapa de riesgos cuando éste así lo requiera.

ii) Registro y gestión de eventos: Gestionar y registrar los eventos, incidentes y fallas para lo cual debe:

- a) Mantener un registro documentado, actualizado, trazable y verificable de los eventos, incidentes, interrupciones, fallas operativas, errores, novedades y/o situaciones que afecten o puedan afectar la prestación del servicio, incluyendo al menos: descripción del evento, causa raíz, impacto, acciones de contención, acciones correctivas y preventivas, responsables y fechas;
- b) Notificar al **BANCO** tan pronto se presente cualquier evento o incidente relevante de manera inmediata, cuando comprometa la continuidad o disponibilidad del servicio o implique afectación al consumidor financiero. Dicho reporte se podrá realizar por parte del **CONTRATISTA** a través de correo electrónico o a través de las visitas de seguimiento en las cuales también se le podrá notificar al supervisor sobre cualquier hallazgo y/o incidente presentado

iii) Continuidad y contingencias: Gestionar la continuidad del negocio y contingencias para lo cual debe:

- a) Contar con planes de contingencia y continuidad del negocio debidamente documentados y probados, de conformidad con la normatividad vigente aplicable, garantizando su capacidad de ejecución frente a eventos que afecten la prestación del servicio;
- b) Dichos planes deberán contemplar, como mínimo responsabilidades, esquema de escalamiento, comunicación de crisis, recursos necesarios, escenarios y estrategias, tiempos objetivo de recuperación y procedimientos de retorno a la operación normal.
- c) El **BANCO** podrá verificar el funcionamiento de dichos planes en lo relacionado con los servicios contratados y el **CONTRATISTA** deberá atender las observaciones y recomendaciones que se generen;

iv) Capacitación: Garantizar que el personal involucrado en la prestación del servicio reciba capacitación mínima una vez al año documentada y evidenciable en gestión del riesgo operacional asociado al servicio, continuidad del negocio y estándares de conducta, ética y trato justo al consumidor financiero, cuando aplique;

v) Trato a consumidores financieros (cuando aplique al objeto y alcance del contrato): Cuando los servicios involucren atención, gestión o interacción con consumidores financieros, el **CONTRATISTA** deberá garantizar el cumplimiento del principio de debida diligencia y trato justo, asegurando como mínimo:

- a) Que los productos, servicios e interacciones sean coherentes con la necesidad del cliente, conforme al alcance del servicio contratado;
- b) El cumplimiento de la promesa de valor y de los niveles de servicio acordados;
- c) El suministro de información clara, suficiente, veraz, transparente y oportuna;
- d) La gestión oportuna, trazable y documentada de las PQRS, incluyendo el escalamiento al **BANCO** cuando corresponda;

vi) Seguimiento y revisión: atender de las visitas, seguimientos, revisiones, pruebas y solicitudes de información que realice el **BANCO** y en los tiempos que este le notifique al **CONTRATISTA**, para verificar el cumplimiento de esta cláusula, aportando evidencias suficientes, consistentes y verificables;

vii) Planes de acción: cuando se identifiquen incumplimientos, hallazgos, debilidades o eventos relevantes en las visitas seguimiento o revisiones, el **CONTRATISTA** deberá formular, ejecutar y reportar a través del supervisor del contrato los planes de acción, con responsables y fechas definidas, informando su avance cuando el **BANCO** lo requiera;

viii) Subcontratación: en caso de que la subcontratación sea aceptada de acuerdo con lo establecido en la cláusula décima séptima, el **CONTRATISTA** deberá exigir, verificar y asegurar que todos los proveedores, subcontratistas o terceros que este utilice para la prestación del servicio objeto del contrato tengan implementado sistemas o modelo de gestión de riesgos y cumplan con la normatividad vigente aplicable y cuenten con sistemas, políticas, procedimientos y controles adecuados para la gestión de los riesgos

de seguridad de la información, ciberseguridad, riesgos operativos, conductas y continuidad del negocio, en función del alcance del servicio tercerizado. Así mismo, el **CONTRATISTA** deberá contar con los soportes, evidencias y documentos que acrediten el cumplimiento y la efectividad de dichos controles por parte de sus proveedores y subcontratistas, conservarlos de manera trazable y presentarlos al **BANCO** cuando este lo requiera, para efectos de verificación, auditoría o seguimiento. En todo caso, el **CONTRATISTA** mantendrá la responsabilidad integral frente al **BANCO** por los riesgos, incumplimientos o afectaciones derivadas de la actuación u omisión de dichos terceros.

IX) Incumplimientos de la cláusula y medidas: El incumplimiento de las obligaciones previstas en esta cláusula dará lugar a las medidas correctivas previstas en el contrato, sin perjuicio de la facultad del **BANCO** de adoptar las acciones de contingencia para proteger la continuidad del servicio, cuando aplique.

PARÁGRAFO- GARANTÍA DE CUMPLIMIENTO Y EVIDENCIAS: El **CONTRATISTA** garantiza al **BANCO** el cumplimiento de las obligaciones previstas en la presente cláusula y se obliga a mantener, durante la vigencia del contrato la documentación, registros y soportes que acrediten la identificación, evaluación, control, registro y gestión de los riesgos asociados a la prestación del servicio. Para tal fin, el **CONTRATISTA** entregará al **BANCO**, en los plazos y formatos que éste solicite, los informes periódicos de gestión de riesgos, reportes de eventos e incidentes, actas de pruebas de continuidad, evidencias de capacitación y los planes de acción con sus avances. Asimismo, el **CONTRATISTA** autoriza al **BANCO** a verificar dichas evidencias mediante revisiones documentales, solicitudes de información y auditorías de cumplimiento, con preaviso razonable, salvo en situaciones de emergencia o incidentes críticos en cuyo caso el **BANCO** podrá actuar sin previo aviso. El incumplimiento en la entrega de las evidencias o la comprobación de información inconsistente podrá activar las medidas correctivas y las acciones correspondientes previstas en el contrato.

(...)