BANCO DAVIVIENDA S.A.
GESTIÓN DEL RIESGO

VERSIÓN: 2 Diciembre 2025

ASUNTOS NORMATIVOS

El DESTINATARIO reconoce y acepta que cumple con los lineamientos y directrices del Banco Davivienda relativos a la administración de riesgos aplicables a la Oferta Mercantil suscrita con el Banco Davivienda y sus filiales.

1.1. AUDITABILIDAD

El DESTINATARIO permitirá al OFERENTE o a terceros autorizados por el OFERENTE, llevar a cabo evaluaciones de auditoría, riesgo, pruebas de seguridad y/o análisis de vulnerabilidades de manera presencial, virtual y/o mediante herramientas tecnológicas, que determine el OFERENTE, con el objetivo de verificar el cumplimiento de controles y procedimientos propios del DESTINATARIO, así como los requisitos incluidos en esta Oferta Mercantil, anexos y demás documentos asociados.

El DESTINATARIO que cuente con certificaciones de auditores externos independientes en temas de sistemas de información en materia de seguridad, disponibilidad, integridad del tratamiento y confidencialidad (SOC2) o relativos al control interno de los informes financieros (SOC1) o sus equivalentes en el país donde se prestará el servicio, los podrá aportar como parte del cumplimiento a esta cláusula.

El OFERENTE podrá comunicar por cualquier medio, la fecha y hora en que se llevará a cabo la(s) respectiva(s) auditoría(s) y/o evaluaciones de forma presencial o virtual.

En caso de presentar un incidente o evento de riesgo materializado el OFERENTE comunicará de manera inmediata al DESTINATARIO la situación identificada a fin de conocer y definir las acciones que se consideren pertinentes para su mitigación.

En caso que el OFERENTE o su tercero delegado, identifiquen incumplimientos en las evaluaciones realizadas al DESTINATARIO, el OFERENTE emitirá el informe respectivo con los planes de acción y/o sanciones a las que haya lugar.

1.2. SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERACIONAL

El DESTINATARIO se obliga a implementar y mantener durante la vigencia de la Oferta Mercantil, un esquema de políticas, gobierno, atribuciones, y procedimientos conforme a su complejidad y realidad operacional, que permitan identificar, valorar, controlar, monitorear y tratar los diferentes tipos de riesgos operacionales inherentes a la prestación de los servicios.

Así mismo, el DESTINATARIO se obliga a mantener actualizada y aprobada por sus instancias de gobierno, la matriz de riesgos con la identificación, análisis, valoración y planes de acción de los riesgos asociados al servicio objeto de la Oferta Mercantil y que permita la gestión de eventos de riesgo que puedan materializarse.

El DESTINATARIO se obliga a suministrar toda la información y/o documentación que sea requerida por el OFERENTE para que este pueda garantizar, atender y responder oportunamente las obligaciones relacionadas con el Sistema de administración de riesgo operacional, otros sistemas de riesgo o aquellas normas que en el futuro la modifiquen, adicionen o aclaren.

1.3. SISTEMA DE ADMINISTRACIÓN DE RIESGO AMBIENTAL Y SOCIAL (SARAS)

El DESTINATARIO declara que conoce y cumple la normatividad vigente en relación con la protección y conservación del medio ambiente, aspectos sociales y laborales de acuerdo con la actividad desarrollada.

Por lo anterior, el DESTINATARIO se obliga a mantener vigente y en regla todas las licencias, permisos, autorizaciones, registros y demás requerimientos legales exigidos por las autoridades competentes que se requieran con ocasión de la ejecución de la Oferta Mercantil. Así mismo declara que conoce y cumple en todos sus aspectos la Ley 2111 de 2021 (sobre los recursos naturales y el medio ambiente para compañías cuyo origen sea Colombia) o las leyes aplicables en materia de cuidado y conservación de los recursos naturales y de medio ambiente vigentes en su país según estas sean modificadas en el tiempo.

El DESTINATARIO será responsable frente al OFERENTE, por la ocurrencia de daños ambientales, sociales y/o generación de pasivos ambientales, que se deriven de la ejecución de la Oferta Mercantil, y asumirá todos los costos de mitigación, compensación y corrección del impacto causado.

En el evento en que por orden de autoridad administrativa, judicial o por voluntad propia el OFERENTE pague suma de dinero derivada de alguna multa, sanción u otro concepto al Estado o a terceros afectados, como consecuencia del incumplimiento de las normas ambientales y sociales por parte del DESTINATARIO, éste último se obliga a reembolsar las sumas de dinero correspondientes al OFERENTE o de lo contrario podrán ser descontadas de los saldos insolutos que existan a favor del DESTINATARIO por los servicios prestados o los bienes suministrados al OFERENTE.

PARÁGRAFO PRIMERO: El DESTINATARIO declara que, en relación con la protección y conservación del medio ambiente, aspectos sociales y laborales, no existe ni ha sido notificado de la existencia de reclamaciones, procesos, demandas, litigios, pasivos, contingencias, sanciones, multas o similares, por el incumplimiento de dicha normatividad, en desarrollo de la Oferta Mercantil.

En caso de materialización de alguno de los anteriores eventos o de cualquier hecho relevante en contra del DESTINATARIO, que pueda afectar su estructura y condición y que pueda afectar o afecte los términos y las

condiciones de la Oferta Mercantil, el DESTINATARIO se obliga a informarlo al OFERENTE de forma inmediata.

PARÁGRAFO SEGUNDO: El DESTINATARIO se obliga a remitir al OFERENTE, informes de cumplimiento, seguimiento o avances de las obligaciones derivadas en materia ambiental, social y laboral cuando el OFERENTE lo requiera, con el fin de evidenciar las actividades de control, compensación o mitigación de impactos negativos, así como permitir y colaborar en las evaluaciones en sitio y controles de seguimiento por parte del OFERENTE o del tercero que este designe.

De igual forma, se obliga a informar al OFERENTE sobre la ocurrencia de daños y/o perjuicios ambientales o sociales o cualquier impacto negativo al ambiente o a la comunidad y/o trabajadores, como consecuencia de la materialización o potencial materialización de los impactos generados por la actividad del DESTINATARIO al entorno, o por los impactos negativos del entorno en la actividad del DESTINATARIO siempre y cuando se evidencie la marca del OFERENTE.

PARÁGRAFO TERCERO: El DESTINATARIO se obliga a respetar los derechos humanos de sus colaboradores, clientes y terceros y en caso de vulneración realizar la reparación de los mismos, con el compromiso de no volver a vulnerarlos.

1.4. PLAN DE CONTINUIDAD Y CONTINGENCIA

El DESTINATARIO se obliga con el OFERENTE a contar con el Sistema de Gestión de Continuidad de Negocio, el cual, debe estar implementado, documentado y certificado, garantizando la prestación de los servicios objeto de la Oferta Mercantil, ante la materialización de escenarios de riesgo que puedan afectar la operación o la disponibilidad de los servicios asociados al objeto de la Oferta,, dicho sistema deberá contemplar mecanismos de respuesta y recuperación frente a eventos de alto impacto incluidos los relacionados con la seguridad de la información.

El DESTINATARIO deberá realizar y mantener pruebas periódicas de sus planes de continuidad y contingencia, por lo menos una vez al año, y remitir los resultados al OFERENTE cuando este así lo requiera. De igual forma, El DESTINATARIO garantizará que los proveedores o subcontratistas vinculados a la prestación del servicio cuenten con mecanismos y planes equivalentes a los exigidos en la presente cláusula.

1.5. ANTIFRAUDE

El DESTINATARIO será el único y exclusivo responsable de cualquier daño, pérdida o perjuicio directo debidamente comprobado, derivado por el fraude económico, exfiltración de información u otros tipos de fraude ocasionados al OFERENTE, sus trabajadores, clientes o terceros y que se materialice durante cualquier etapa de la Oferta Mercantil.

El DESTINATARIO se obliga a implementar, monitorear y actualizar los controles necesarios basados en los estándares y mejores prácticas de la industria, con el fin de evitar la ocurrencia de fraudes de acuerdo con los niveles de riesgo de la operación, garantizando la debida diligencia y cuidado profesional.

1.6. APLICABILIDAD DE MEJORES PRÁCTICAS

EL DESTINATARIO como compañía especializada, profesional y experta en los servicios objeto de la Oferta Mercantil, se obliga a emplear las mejores prácticas establecidas en los estándares nacionales e internacionales que apliquen al objeto de la Oferta Mercantil. El DESTINATARIO garantiza que sus Sistemas de Gestión asociados al objeto de la Oferta Mercantil se encuentran plenamente alineados e integrados a dichos estándares y mejores prácticas.

Para Contratos donde se haga uso de alguna tecnología, el DESTINATARIO se obliga a emplear los estándares y mejores prácticas en seguridad, incluyendo sin limitar los estándares OWASP (Open Web Application Security Project), OSSTMM (Open Source Security Testing Methodology Manual) y demás estándares aplicables como la serie NIST (Nacional Institute of Standards and Technology), ISO 27000 entre otras.

1.7. CUSTODIA Y MANEJO DE BASES DE DATOS Y/O INFORMACIÓN DEL BANCO DAVIVIENDA

En caso que el Banco Davivienda entregue al DESTINATARIO algún tipo de información o Bases de Datos durante la vigencia de la Oferta Mercantil, este se obliga a custodiar las bases de datos entregadas por el OFERENTE y destinarlas exclusivamente para la ejecución de la Oferta Mercantil.

El DESTINATARIO debe realizar el cifrado en tránsito, reposo y uso de la información que llegare a recibir por parte del OFERENTE y que con ocasión de la Oferta Mercantil deba custodiar y garantizará que las bases de datos entregadas, permanezcan cifradas incluso para el manejo interno por parte del DESTINATARIO.

El DESTINATARIO debe contar con herramientas de seguridad perimetral y herramientas que permitan el monitoreo y detección para prevenir la pérdida de datos y/o la fuga de información.

1.8. INFIDELIDAD FINANCIERA

El DESTINATARIO será responsable ante el OFERENTE en los casos en que sus empleados, ex empleados, asociados, contratistas o subcontratistas incurran en situaciones que puedan considerarse como infidelidad financiera y que configuren un daño, pérdida o perjuicio para el OFERENTE, terceros y/o los consumidores financieros. Para efectos de esta cláusula se entenderá como infidelidad financiera todo acto en el que se tome provecho de la información, procedimientos, *know how*, y cualquier actividad, responsabilidad u obligación establecida en esta Oferta Mercantil, para la comisión de infracciones al sistema financiero, delitos contra el patrimonio económico y cualquier actividad ilícita de acuerdo con la legislación colombiana.

1.9. SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Teniendo en cuenta que la información del OFERENTE es uno de sus activos más importantes, el DESTINATARIO que para la prestación del servicio objeto de la Oferta Mercantil conozca, reciba, genere, procese, almacene o recolecte información se obliga a:

1. Establecer y mantener un programa de seguridad de la información y ciberseguridad alineado a mejores prácticas internacionales como ISO 27001, u otro estándar aplicable que incluya pero no se limite a aspectos como seguridad de la información para elementos físicos, digitales, virtuales y ciberespacio independiente de su tránsito y/o ubicación. Asimismo, capacitar a sus empleados y terceros, al menos una vez al año en temas de seguridad de la información y ciberseguridad y procedimientos para la protección de manera anticipada contra amenazas y/o riesgos.

Si el DESTINATARIO posee una evaluación de riesgos, como SOC2, o tiene la certificación ISO27001, deberá proporcionar al OFERENTE el documento que acredite la realización de dicho proceso y mantenerlo vigente durante la validez de la Oferta Mercantil.

2. Definir e implementar un procedimiento de reporte, registro, investigación y respuesta ante materialización de eventos, amenazas e incidentes de seguridad y/o ciberseguridad. El procedimiento debe ser divulgado y sensibilizado a todo el personal que prestará el servicio. El procedimiento debe establecer los responsables, las definiciones de incidentes y las acciones a tomar por parte del DESTINATARIO ; entre ellas las actividades de cooperación en la respuesta, contención e investigación del incidente con el OFERENTE una vez se detecten eventos, amenazas, incidentes de seguridad o ciberseguridad. Así mismo debe verificar que se mantenga un registro de los eventos (causa raíz del incidente, los efectos e impactos causados, los detalles sobre el plan de respuesta y cierre, entre otros) y mantener las evidencias digitales, custodia y disponibilidad de las mismas, y los planes de acción para evitar nuevas materializaciones.

   En caso que el DESTINATARIO identifique una amenaza o la materialización de cualquier tipo de evento de seguridad de la información y/o ciberseguridad que atente o pudiese afectar la reputación, la operación o cualquier tipo de afectación al OFERENTE en el servicio contratado, el DESTINATARIO se obliga a reportar inmediatamente al correo electrónico *iris@davivienda.com* y al supervisor de la Oferta Mercantil del OFERENTE para que en conjunto se tomen las acciones pertinentes.

3. Para las ofertas mercantiles que dentro de la prestación de su servicio reciban, almacenen, procesen, entreguen o transmitan datos de titulares de tarjetas y/o datos confidenciales de autenticación, de acuerdo al estándar PCI DSS (Payment Card Industry Data Security Standard), además de los requisitos anteriormente expuestos, el DESTINATARIO se obliga mantener vigente la certificación con los requisitos de la regulación PCI DSS (Payment Card Industry Data Security Standard) que apliquen al proceso contratado por el OFERENTE y enviar anualmente al Supervisor de la Oferta Mercantil del

OFERENTE, la certificación vigente PCI/DSS expedida por un QSA (Qualified Security Assessor) avalado por PCI/SSC (Security Standard council).

4. Para las Ofertas Mercantiles que incluyan cualquier tipo de servicio alojado en la nube, el DESTINATARIO se obliga a cumplir con la normativa vigente, los estándares y mejores prácticas definidas en la industria, así como las políticas establecidas por el OFERENTE para este fin, las cuales se incorporan como anexo a la Oferta Mercantil y hace parte integral de la misma.

5. El DESTINATARIO, debe realizar pruebas de vulnerabilidades en todos los componentes comprometidos en la prestación del servicio objeto de la Oferta Mercantil con una periodicidad mínima de dos (2) veces por año, con una diferencia de al menos seis meses entre cada prueba Así mismo debe realizar al menos una (1) vez al año un Ethical Hacking durante la vigencia de la Oferta Mercantil, y siempre que se realicen cambios en la infraestructura tecnológica que soporta el servicio objeto de la Oferta Mercantil. El DESTINATARIO se obliga a dar cierre a las vulnerabilidades identificadas de acuerdo a su criticidad en un periodo no mayor a: críticas/altas: 30 días, medias/severas: 60 días y moderadas o bajas: 90 días. Así mismo debe realizar pruebas trimestrales sobre las aplicaciones.

6. En caso que el OFERENTE considere necesario, podrá solicitar una certificación sobre la ejecución de las pruebas y/o plan de remediación de las vulnerabilidades detectadas. Adicionalmente, el OFERENTE podrá compartir con el DESTINATARIO el informe con los hallazgos identificados producto de sus evaluaciones o monitoreos de seguridad de la información y ciberseguridad, las cuales deberán ser remediadas en los mismos tiempos mencionados anteriormente.

7. El DESTINATARIO debe reportar al Supervisor de la Oferta Mercantil en los casos en que se presenten incumplimientos en los tiempos de remediación de las vulnerabilidades críticas y altas sobre la infraestructura que directa o indirectamente afecte la prestación del servicio incluyendo las fechas de cierre de las mismas. El DESTINATARIO deberá remitir la certificación correspondiente una vez hayan sido subsanadas.

8. El DESTINATARIO, se obliga a conocer y cumplir los lineamientos y directrices de las (i)Políticas y (ii)Guía de Seguridad de la Información para Terceros del OFERENTE las cuales se encuentran publicadas en *https://proveedores.davivienda.com/gestion-de-riesgo/* que apliquen a la Oferta Mercantil. Así mismo, hará un uso pertinente y estricto de las plataformas tecnológicas que el OFERENTE ponga a disposición para la prestación del servicio objeto de la Oferta Mercantil, absteniéndose de interferir en otras redes, enviar o propagar virus informáticos o realizar cualquier actividad que vaya en contra de ésta política y la normativa vigente sobre el particular.

9. Notificar al Supervisor de la Oferta Mercantil del BANCO DAVIVIENDA aquellas modificaciones en sus procedimientos de seguridad de la información y ciberseguridad, incluyendo seguridad física, y tecnológicos que afecten las condiciones de seguridad del servicio inicialmente pactadas, las cuales

deberán contar con la aprobación del OFERENTE, aprobación que en el evento de otorgarse, se expedirá 15 días después de la notificación de dicho cambio.

10. En el evento en que el DESTINATARIO almacene, custodie, capture, procese o transforme información de propiedad del OFERENTE, se obliga a contar con una política de gestión de accesos que garantice, como mínimo, i) el principio de mínimo privilegio (Principio del Menor Privilegio) para todo los funcionarios destinados al desarrollo del objeto de la Oferta Mercantil, ii) la obligatoriedad de usar Autenticación Multifactor (MFA) para todos los accesos a las plataformas o herramientas requeridas para el desarrollo directo o indirecto del servicio y iii) realizar revisiones periódicas (como mínimo de forma semestral) de las cuentas y accesos provistos para asegurar que sigan siendo necesarios (recertificación) iv) Retirar los accesos y/o permisos de los funcionarios del DESTINATARIO que no se encuentren ejecutando actividades propias del servicio objeto de la Oferta Mercantil, incluyendo una validación periódica del cumplimiento de esta actividad (como mínimo de forma mensual).

11. En el evento en que el OFERENTE i) autorice la subcontratación de actividades propias del objeto de la Oferta Mercantil o si los servicios de una Oferta Mercantil son prestados por parte de un canal debidamente autorizado y ii) con relación al desarrollo de estas actividades exista custodia, captura, procesamiento o transformación de información de propiedad del OFERENTE, el DESTINATARIO garantizará que el subcontratista del servicio y/o actividad o el fabricante, cumplen con las disposiciones establecidas en la presente cláusula.

12. El DESTINATARIO deberá devolver la información física o digital de propiedad del OFERENTE, entregada o generada en virtud del servicio contratado, a la terminación del contrato y/o cuando así lo solicite el OFERENTE. Sin perjuicio de lo anterior, EL DESTINATARIO se obliga a realizar el borrado a bajo nivel de toda la información que se haya intercambiado física o lógicamente y esté almacenada en su infraestructura tecnológica o de sus Contratistas dando cumplimiento a los lineamientos definidos en sus normas de seguridad de la información.

1.10. DESARROLLO DE SOFTWARE (CÓDIGO FUENTE)

El DESTINATARIO que preste servicios de desarrollo de software y preste este servicio para el OFERENTE, debe contar con un procedimiento implementado para el desarrollo de aplicaciones seguras Secure System Development Life Cycle (S-SDLC), lo cual deberá ser evidenciado con la entrega de informes de revisión de código fuente tipo SAST (Secure Análisis Static Testing) emitidos por un tercero independiente que cuente con experiencia certificada que lo acredite como experto en conocimiento en lenguajes de programación y en seguridad para el desarrollo de software.

Cada versión del software que vaya a ser desplegada en el ambiente de producción deberá estar acompañada del respectivo informe tipo SAST, sobre el cual, el supervisor de la Oferta Mercantil del OFERENTE emitirá el aval o rechazo para el despliegue. En caso que el DESTINATARIO cuente con el informe tipo DAST (Dynamic Application Security Testing), también deberá entregarlo al Supervisor de la Oferta Mercantil del Banco Davivienda.

La revisión deberá incluir como mínimo: identificación de usuarios, autenticación y protección de datos, autorizaciones de acceso, lectores de formato, operaciones no seguras en cadenas, búferes y punteros, códigos de conversión de datos, lógica empleada en la interpretación de datos, código involucrado en la generación de mensajes de error, validación de no inclusión de código malicioso,pruebas unitarias, de integración y funcionales. Uso de Infraestructura como código (IaC) para la provisión y configuración y gestión de la infraestructura si se requiere, Gestión de dependencias con escaneo de vulnerabilidades en librerías. Control de versiones, integración y entrega continua haciendo uso de pipeline de automatización así como el cumplimiento de normas, estándares determinados por el OFERENTE y mejores prácticas internacionales para el desarrollo de software como OWASP (Open Web Application Security Project), OSSTMM (Open Source Security Testing Methodology Manual) y demás estándares aplicables como la serie NIST (National Institute of Standards and Technology), ISO27000 entre otras, las cuales deben ser acordadas con el OFERENTE e incorporadas como anexo a la Oferta Mercantil.

Con el fin de garantizar el cumplimiento de los requisitos anteriormente descritos, el DESTINATARIO se obliga a entregar al Supervisor de la Oferta Mercantil una certificación con la descripción detallada del procedimiento de desarrollo seguro, las validaciones realizadas y el resultado del estado de las vulnerabilidades encontradas, las cuales deben estar remediadas para el aval respectivo por parte del OFERENTE.

En los casos en los cuales las Partes acuerden que el DESTINATARIO entregará el Código Fuente al DESTINATARIO, este último, se reserva el derecho a realizar las revisiones que considere necesarias en cualquier tiempo. En el caso en el que realizada la validación, el OFERENTE identifique algún incumplimiento de los requisitos y estándares anteriormente definidos, el Supervisor de la Oferta Mercantil informará por medio escrito al DESTINATARIO A los ajustes, términos y condiciones requeridos, sin perjuicio de las acciones que pueda determinar el OFERENTE como medida. Así mismo, Las Partes deberán incluir el procedimiento de entrega del Código Fuente en el Acuerdo de Niveles de Servicio o en documento anexo que hará parte integral de la Oferta Mercantil.

En cualquier caso, el DESTINATARIO se obliga a prestar el servicio mediante un proceso de desarrollo seguro, a entregar el software libre de toda brecha de seguridad, vulnerabilidad, código malicioso y a asumir la responsabilidad por todo defecto asociado a seguridad y calidad del software que genere pérdidas, daños o perjuicios al OFERENTE. De igual forma el DESTINATARIO se obliga a cumplir con las obligaciones definidas en el anexo de seguridad para desarrollo de software el cual hace parte integral de la Oferta Mercantil.

1.11. DISPOSICIÓN FINAL DE RESIDUOS

El DESTINATARIO que para la prestación de los servicios objeto de la Oferta Mercantil utilice elementos muebles o los genere por la ejecución del mismo se obliga a realizar su disposición final de acuerdo con la normativa vigente.

La disposición final de residuos se debe realizar sobre todos aquellos residuos peligrosos y/o residuos de aparatos eléctricos y electrónicos y/u otro tipo de residuos. Se entiende por "proceso de disposición final", el aislamiento y confinación de los residuos o desechos peligrosos, en especial los no aprovechables, en lugares especialmente seleccionados, diseñados y debidamente autorizados, para evitar la contaminación y los daños o riesgos a la salud humana y para el medio ambiente. El OFERENTE podrá solicitar cuando lo requiera una certificación de la realización del proceso de disposición final de residuos con la discriminación de los objetos a los cuales se les aplicó este procedimiento por parte del DESTINATARIO.

CERTIFICACIÓN RESIDUOS POSCONSUMO: El OFERENTE podrá solicitar, en caso que lo requiera, el CERTIFICADO DE DISPOSICIÓN FINAL DE RESIDUOS POSCONSUMO debidamente diligenciado y firmado por el Representante Legal de la entidad Gestora del Programa Posconsumo de productores o importadores correspondiente.

En caso de controversia entre las Partes, la interpretación de la presente cláusula se ceñirá de acuerdo a las definiciones y alcances dados por la normativa ambiental vigente al momento de la controversia.

1.12. DISPOSICIÓN FINAL DE RESIDUOS PELIGROSOS

El DESTINATARIO se obliga a realizar la gestión para la disposición final adecuada de los residuos peligrosos, de los residuos de aparatos eléctricos y electrónicos-RAEE- y de los residuos posconsumo que resulten de la prestación del servicio objeto del contrato, de acuerdo con la normativa vigente.

PARÁGRAFO PRIMERO: La presente cláusula aplicará en caso que el DESTINATARIO preste algún servicio (s) y/o entregue algún tipo de bien (es) relacionado (s) con la siguiente lista de elementos:

I. Tubos de rayos catódicos (bombillos fluorescentes).
II. Acumuladores de UPS, plantas de generación de energía, inversores (Baterías plomo-ácido).
III. Transformadores obsoletos (posible contaminación con PCB).
IV. Computadores y periféricos.
V. Cartuchos de impresoras y/o impresión.

La anterior lista no es taxativa, y en efecto, será extensiva a todos aquellos elementos que la normativa ambiental exija.

PARÁGRAFO SEGUNDO: CERTIFICACIONES

CERTIFICACIÓN RESIDUOS PELIGROSOS: El OFERENTE podrá solicitar, en caso que lo requiera, el CERTIFICADO DE DISPOSICIÓN FINAL DE RESIDUOS PELIGROSOS emitido por la entidad Receptora (entidad que lleva a cabo el proceso de disposición final de residuos peligrosos) según lo dispuesto en el Decreto 4741 de 2005.

CERTIFICACIÓN RESIDUOS POSCONSUMO: El DESTINATARIO podrá solicitar, en caso que lo requiera, el CERTIFICADO DE DISPOSICIÓN FINAL DE RESIDUOS POSCONSUMO debidamente diligenciado y firmado por el Representante Legal de la entidad Gestora del Programa Posconsumo de productores o importadores correspondiente.

En caso de controversia entre las Partes, la interpretación de la presente cláusula se ceñirá de acuerdo a las definiciones y alcances dados por la normativa ambiental vigente al momento de la controversia.

1.13. SERVICIOS NO TECNOLÓGICOS

El DESTINATARIO que para la ejecución del servicio contratado no requiera utilizar sistemas de información tecnológicos a través de los cuales se administre, almacene y/o custodie información de los clientes, transacciones y/o datos del OFERENTE, se abstendrá de implementarlos o usarlos durante la vigencia de la Oferta Mercantil. En los eventos en que se requiera este tipo de sistemas, la autorización para su utilización deberá ser emitida expresamente y por escrito por parte del OFERENTE.

En caso que el OFERENTE identifique que el DESTINATARIO CONTRATISTA ha incumplido la presente cláusula, podrá terminar inmediatamente la Oferta Mercantil de manera unilateral sin lugar al pago de multa, penalidad o indemnización alguna, sin perjuicio de las acciones legales a las qué hubiere lugar para obtener el reconocimiento de los daños, pérdidas y/o perjuicios ocasionados al OFERENTE por el incumplimiento.

1.14. INTERRUPCIÓN DE LOS SERVICIOS EN CANALES

El DESTINATARIO que preste servicios que directa o indirectamente se relacionen con canales transaccionales se obliga a informar al OFERENTE con quince (15) días de antelación, sobre los mantenimientos preventivos a realizar en relación con estos canales, las modificaciones y/o actualizaciones técnicas o tecnológicas que puedan generar una interrupción en la prestación del servicio y/o afectar la realización de operaciones de clientes y/o usuarios del OFERENTE.

El DESTINATARIO debe informar por escrito al Supervisor de la Oferta Mercantil del OFERENTE, el detalle de las modificaciones y/o actualizaciones técnicas o tecnológicas a realizar, el tiempo estimado del procedimiento, operaciones que no se puedan realizar, canales y servicios que se afectarán, canales alternativos, y aquella información relevante para el OFERENTE.

Cuando se presente un evento o incidente que impida la realización de operaciones de clientes y/o usuarios del OFERENTE por una hora o más, el DESTINATARIO debe informar de manera inmediata y por escrito al Supervisor de la Oferta Mercantil del OFERENTE, la descripción detallada del evento, operaciones afectadas, la fecha y hora estimada en que se restablecerá la prestación del servicio, operaciones que no se pueden realizar, canales y servicios afectados, y aquella información relevante para el OFERENTE con el objetivo de orientar a clientes y/o usuarios.

Si como consecuencia de eventos o incidentes a cargo del DESTINATARIO se causan daños, pérdidas o perjuicios al OFERENTE o a los consumidores financieros por la afectación, en la realización de operaciones, acceso a canales transaccionales y en general la prestación de servicios a clientes y/o usuarios del OFERENTE, el DESTINATARIO asumirá dichos daños, pérdidas o perjuicios que se generen.

El DESTINATARIO autoriza al OFERENTE para que deduzca estos valores de los pagos pendientes por los servicios prestados.

1.15. SAC - PRESTACIÓN DE SERVICIOS DE TERCEROS CON IMPACTO DIRECTO O INDIRECTO EN EL CONSUMIDOR FINANCIERO DEL BANCO DAVIVIENDA

El DESTINATARIO que para la ejecución del servicio contratado deba realizar interacciones directas o indirectas con clientes y/o usuarios del OFERENTE se obliga a cumplir con la normativa vigente y a garantizar los derechos del consumidor / Cliente / Usuarioo, así como un servicio que brinde experiencias sencillas, confiables y amigables, para que en el desarrollo de las actividades contratadas, se garantice el trato justo, la debida diligencia, la transparencia e información cierta, suficiente y oportuna, manejo adecuado de conflicto de intereses y/o incentivos asociados a la colocación de productos en los casos que aplique de acuerdo con el objeto del contrato. Así mismo, debe realizar mediciones de satisfacción y experiencia que permitan retroalimentar y mejorar los esquemas de atención que aseguren la calidad y oportunidad del servicio ofrecido de acuerdo con las políticas de servicio del OFERENTE.