Partes	
Responsable	Junta Nacional de Calificación de Invalidez -JNCI-
ID/NIT	830.026.324-5
Encargado	UT NAFILEX DOC 2026
ID/NIT	N/A
Finalidad	PRESTACIÓN DE SERVICIOS PARA REALIZAR LA REVISIÓN, AJUSTES, COTE LEVANTAMIENTO DE INFORMACIÓN NECESARIA PARA EL DESARROLLO CONVALIDACIÓN POSITIVA DE LAS TRD DE LA JUNTA NACIONAL DE CALIFICACIÓN INVALIDEZ ANTE EL AGN.
Contrato No.	CTO-017-JNCI-2026

DISPOSICIONES GENERALES:

i. NATURALEZA DEL ACUERDO: Este instrumento funciona como Contrato de Transmisión de Datos Personales (Ley 1581/2012 y D.1074/2015), además de NDA. El Encargado trata datos por cuenta del Responsable, sin adquirir titularidad.

ii. El tratamiento se limitará exclusivamente al cumplimiento de la finalidad contractual indicada, aplicando el principio de minimización de datos y, cuando sea técnicamente viable, pseudonimización o enmascaramiento. EL ENCARGADO actuará únicamente bajo instrucciones documentadas de EL RESPONSABLE.

iii. Queda prohibida la subcontratación de actividades de tratamiento sin autorización previa, expresa y escrita de EL RESPONSABLE. Todo subencargado quedará vinculado por obligaciones equivalentes o más estrictas a las aquí pactadas, incluyendo medidas de seguridad, auditoría y localización del tratamiento.

iv. Cuando existan transferencias o transmisiones internacionales de datos personales, las Partes observarán las reglas sobre nivel adecuado de protección, garantías apropiadas y trámites/registro que correspondan; EL ENCARGADO informará previamente rutas de flujo, países y subencargados involucrados, y apoyará a EL RESPONSABLE en los procedimientos ante la autoridad competente.

v. EL ENCARGADO implementará y mantendrá medidas técnicas, organizativas y jurídicas adecuadas para preservar la confidencialidad, integridad, disponibilidad y resiliencia de la información, detalladas en el Anexo de Medidas de Seguridad, que forma parte integral de este Contrato.

vi. En caso de incidente de seguridad que comprometa datos personales, EL ENCARGADO notificará a EL RESPONSABLE sin dilación indebida y, en todo caso, dentro de las veinticuatro (24) horas siguientes a su detección, aportando un informe técnico inicial en un plazo no mayor a setenta y dos (72) horas, y colaborará para que EL RESPONSABLE cumpla con los reportes y actuaciones que exija la autoridad de control dentro de los plazos legales.

vii. Toda petición, queja, reclamo o consulta de titulares recibida por EL ENCARGADO será trasladada a EL RESPONSABLE dentro de los dos (2) días hábiles siguientes, adjuntando evidencias y sin resolver de fondo salvo instrucción expresa.

viii. EL RESPONSABLE podrá auditar el cumplimiento de este Contrato y del Anexo de Medidas, directamente o a través de terceros, con preaviso razonable y sin afectar secretos industriales; EL ENCARGADO atenderá las auditorías y ejecutará los planes de remediación acordados.

ix. A la terminación del Contrato, EL ENCARGADO realizará la devolución o eliminación de los datos

personales y la destrucción segura de copias y respaldos, salvo conservación legal, y expedirá certificación escrita de dichas actuaciones; los datos permanecerán bloqueados mientras subsistan responsabilidades.

x. Cada Parte será responsable por el incumplimiento de sus obligaciones; en ningún caso se entenderán exoneradas las responsabilidades del RESPONSABLE frente a los titulares o la autoridad por el tratamiento efectuado por EL ENCARGADO.

De acuerdo con lo anterior, las partes establecen que:

Las partes suscriben el presente Acuerdo de Confidencialidad para el Tratamiento y Transmisión de Datos Personales (el "Acuerdo") para regular el acceso y tratamiento de información a cargo de EL RESPONSABLE por parte de EL ENCARGADO, bajo instrucciones documentadas.

Este Acuerdo fija obligaciones sobre confidencialidad, seguridad, subencargados, gestión de incidentes, atención de titulares, auditoría y cierre del tratamiento, conforme a la Ley 1581 de 2012, el Decreto 1074 de 2015 y las directrices de la SIC.

Los Anexos forman parte integral del Acuerdo.

TRATAMIENTO DE LOS DATOS PERSONALES

LAS PARTES se obligan a realizar el tratamiento de los datos personales objeto del presente acuerdo, de acuerdo con las siguientes condiciones:

I. **Uso permitido y comunicaciones.** EL ENCARGADO no utilizará los datos personales para fines propios ni distintos a los instruidos por EL RESPONSABLE y no realizará envíos masivos de comunicaciones no solicitadas. En ningún caso fomentará actividades contrarias a la ley o a la moral.

II. **Copias y conservación**. EL ENCARGADO no hará copias de las bases de datos salvo las estrictamente necesarias para continuidad/seguridad (p. ej., respaldos), que estarán cifradas, con registro de copias y plazos de retención acordes al Contrato y la ley. Prohibida su descarga a dispositivos no autorizados.

III. **Confidencialidad.** EL ENCARGADO mantendrá la reserva absoluta de la información a la que acceda, obligando a su personal y subcontratistas mediante compromisos escritos. Este deber pervive tras la terminación del Contrato.

IV. **Alcance y minimización.** El Tratamiento se limitará a los datos y campos estrictamente necesarios para la correcta ejecución del Contrato. Cuando sea viable, se preferirá acceso controlado a sistemas del RESPONSABLE y/o pseudonimización/enmascaramiento en lugar de remitir bases completas.

V. **Transmisión segura**. El envío o acceso remoto para fines de mantenimiento se realizará exclusivamente mediante herramientas y canales seguros que EL RESPONSABLE tenga establecidos (p. ej., VPN/SFTP/portales con cifrado), quedando prohibidos canales no autorizados.

VI. **Licitud y calidad del origen.** EL RESPONSABLE declara que los datos han sido obtenidos lícitamente y conforme a la normativa aplicable. EL ENCARGADO informará a EL RESPONSABLE cualquier inconsistencia o desactualización que identifique durante la prestación, para que este adopte las medidas que correspondan. Se suprime cualquier exoneración general de responsabilidad del RESPONSABLE frente a titulares o autoridad.

VII. **Marco normativo y políticas**. El Tratamiento se sujetará a (i) las autorizaciones y

finalidades definidas por EL RESPONSABLE, (ii) la Política de Tratamiento de EL RESPONSABLE, y (iii) la normativa aplicable. Las políticas internas de EL ENCARGADO no ampliarán finalidades ni derechos y se aplicarán solo como soporte de cumplimiento.

VIII. **Responsabilidad.** Cada Parte responderá por el incumplimiento de sus obligaciones legales y contractuales en materia de protección de datos, incluyendo los actos u omisiones de su personal y subencargados debidamente autorizados. EL RESPONSABLE mantiene su responsabilidad frente a los titulares y la autoridad por el tratamiento realizado por EL ENCARGADO.

IX. **Indemnidad.** La Parte que incurra en incumplimiento deberá mantener indemne a la Parte afectada por los perjuicios directos causados, incluidas sanciones, costos y gastos razonables derivados del incumplimiento, en la medida permitida por la ley y sin perjuicio de los demás remedios contractuales.

TRANSMISIÓN Y/O TRANSFERENCIA DE DATOS

Las PARTES manifiestan que la JUNTA NACIONAL DE CALIFICACION DE INVALIDEZ (por sus siglas JNCI o el RESPONSABLE) es responsable de los datos de carácter personal contenidos y/o tratados en sus sistemas de información, y ha decidido contratar los servicios del encargado del tratamiento, consistentes en las actividades que se enmarquen en el contrato de prestación de servicios suscrito por las partes.

Que para la ejecución de dichos servicios resulta necesario que el encargado del tratamiento acceda y/o trate datos personales contenidos en las bases de datos de las que es responsable la JNCI.

Para la ejecución de los servicios descritos anteriormente, la JNCI autoriza al encargado del tratamiento el manejo de los datos personales que la JNCI le suministre. De acuerdo con la relación contractual de las partes.

El encargado del tratamiento únicamente tratará los datos conforme a las instrucciones que reciba expresamente de la JNCI o las actividades que se enmarquen en el contrato de prestación de servicios suscrito por las partes, y no los destinará, aplicará o utilizará con fin distinto al que figure en el presente acuerdo o de cualquier otra forma que suponga un incumplimiento de las instrucciones expresas que la JNCI le proporcione o lo indicado en el contrato de servicios.

De igual modo, el encargado del tratamiento se compromete a no revelar, transferir, ceder o de otra forma comunicar las bases de datos o datos contenidos en ellas, ya sea verbalmente o por escrito, por medios electrónicos, papel o mediante acceso informático, ni siquiera para su conservación, a otras personas que no estén autorizadas o que en virtud de sus servicios deban conocerlas.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa de la JNCI, comunique los datos a un tercero designado por aquel, al que hubiera encomendado la prestación de un servicio.

De acuerdo con lo dispuesto en el artículo cuarto (4) literal h) de la Ley 1581 de 2012, el encargado del tratamiento se compromete y obliga a guardar secreto de todos los datos de carácter personal que conozca y a los que tenga acceso en virtud del presente contrato. Igualmente, custodiará e impedirá el

acceso a los datos de carácter personal a cualquier usuario no autorizado o persona ajena al encargado del tratamiento. Las anteriores obligaciones se extienden en cualquier fase del tratamiento que de esos datos pudiera realizarse y subsistirá aún después de terminados los mismos.

El encargado del tratamiento pondrá en conocimiento del personal a su servicio las obligaciones recogidas en el presente contrato, cerciorándose, mediante la adopción de las medidas pertinentes, de que se acata su contenido.

El encargado del tratamiento se obliga a respetar todas las obligaciones que pudieran corresponderle con arreglo a la normativa en materia de protección de datos.

De igual modo, manifiesta tener implantadas las medidas de seguridad para los datos de carácter personal y en especial los datos sensibles y garantiza el mantenimiento de estas medidas de seguridad, así como cualesquiera otras que le fueren impuestas, de índole técnica y organizativa y siempre que sean acordadas por las partes o sean necesarias y requeridas por la normatividad nacional, con la finalidad de evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. El responsable del tratamiento facilitará, a solicitud del encargado del tratamiento, un extracto de las medidas de seguridad que debe acatar en cumplimiento de las obligaciones descritas en esta cláusula.

El encargado del tratamiento se compromete a comunicar a el RESPONSABLE cualquier incidencia que se produzca en ejecución del presente contrato, especialmente aquellas relacionadas con el ejercicio de derechos de consulta y reclamos por parte de los titulares de los datos. Esta comunicación deberá llevarse a cabo dentro del plazo máximo de DOS (2) días contados desde la fecha en que se hubiese producido la incidencia o hubiese tenido conocimiento de esta.

El responsable y/o encargado del tratamiento no podrá subcontratar con terceros la realización de ningún tratamiento que le hubiera encomendado el RESPONSABLE, salvo que hubiera obtenido autorización previa, expresa y por escrito para ello; la cual, de existir, contendrá los extremos exigidos por la normativa sobre protección de datos, y se anexará al presente contrato.

Una vez cumplida o resuelta la prestación contractual acordada entre el RESPONSABLE y el ENCARGADO del tratamiento, que justifica el acceso a los datos de carácter personal, los datos de carácter personal serán destruidos o devueltos a la JNCI al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de estos a la JNCI, o al responsable y/o encargado del tratamiento que se haya designado al efecto, garantizando dicha conservación.

El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con la JNCI.

PARÁGRAFO UNO — Transferencia internacional y copias de seguridad en nube. Cualquier transferencia o transmisión internacional de información (incluidos datos personales) vinculada al Servicio solo procederá cuando: (i) el país de destino cuente con nivel adecuado de protección o, en su defecto,

existan garantías apropiadas (p. ej., cláusulas contractuales, normas corporativas vinculantes) y, cuando sea exigible, previa declaración de conformidad ante la autoridad competente; y (ii) medie autorización previa y escrita de EL RESPONSABLE. EL ENCARGADO informará por escrito, antes de iniciar cualquier flujo, los países/regiones, subencargados involucrados y la finalidad del tratamiento, y apoyará los registros/actualizaciones que correspondan. Las copias de seguridad y demás componentes en nube se alojarán únicamente en [proveedores/servicios] y [regiones/países] preaprobados por EL RESPONSABLE, con cifrado en tránsito y en reposo, custodia segura de llaves, segregación lógica entre clientes y controles de acceso bajo privilegio mínimo; queda prohibida la replicación, sincronización o tratamiento fuera de las regiones aprobadas, así como la descarga a dispositivos no autorizados. Todo subencargado de nube requerirá autorización previa y quedará sujeto a obligaciones no menos estrictas que las aquí pactadas (flujo-down). EL ENCARGADO mantendrá registro de ubicaciones y restauraciones, cumplirá los RPO/RTO definidos, y no usará los respaldos para fines distintos al Servicio. A la terminación, procederá a la devolución o supresión de respaldos y réplicas (incluidos metadatos) y entregará certificación de borrado seguro en [30] días hábiles una vez hayan culminado los 5 años obligatorios de almacenamiento de información; mientras subsistan obligaciones legales, los datos permanecerán bloqueados. Los accesos remotos de soporte realizados desde el exterior se considerarán transferencia/transmisión internacional y se sujetarán íntegramente a lo previsto en este parágrafo.

OBLIGACIONES DEL ENCARGADO

i. Instrucciones y ley. Tratará los datos exclusivamente según instrucciones documentadas de EL RESPONSABLE y la normativa aplicable, sin fines propios ni ampliación de finalidades.
ii. Confidencialidad. Mantendrá reserva absoluta; acceso bajo necesidad de conocer y compromisos escritos de su personal/subencargados.
iii. Seguridad. Implementará las medidas del Anexo A (cifrado en tránsito/reposo, control de acceso con MFA, registros y monitoreo, gestión de vulnerabilidades, backups cifrados y DRP).
iv. Copias y soportes. No hará copias salvo las estrictamente necesarias (operación/seguridad), cifradas, con registro y plazos de retención. Prohibida la descarga a dispositivos/canales no autorizados.
v. Subencargados. Requieren autorización previa y escrita; quedarán sujetos a obligaciones no menos estrictas (flujo-down). Informará altas/cambios con antelación razonable.
vi. Incidentes. Notificará a EL RESPONSABLE ≤ 48 horas desde la detección y entregará informe inicial en ≤ 72 horas; cooperará para el reporte a la SIC dentro de los 15 días hábiles y para la remediación.
vii. Derechos de titulares. Trasladará a EL RESPONSABLE cualquier consulta o reclamo en ≤ 2 días hábiles, con evidencias, sin responder de fondo salvo instrucción.
viii. Transferencias/nube. No realizará transferencias o transmisiones internacionales ni alojará/replicará datos en nubes/zonas no preaprobadas por EL RESPONSABLE, salvo con garantías y autorización (ver Parágrafo de Transferencia y Nube).
ix. Requerimientos de autoridad. Avisará previamente a EL RESPONSABLE (si la ley lo permite) y limitará la revelación a lo estrictamente exigido, conservando evidencia.
x. Auditorías. Permitirá auditoría (in situ o remota) con preaviso razonable y ejecutará planes de remediación acordados.

xi. Cierre. A la terminación, devolverá o eliminará datos y respaldos, y emitirá certificación en ≤ 10 días hábiles; mantendrá bloqueo si persisten obligaciones legales.

xii. Accountability. Mantendrá registros de actividades y capacitación periódica del personal con acceso.

OBLIGACIONES DEL RESPONSABLE

i. Instrucciones y punto de contacto. Entregará instrucciones documentadas y actualizadas y designará contacto para protección de datos/seguridad.

ii. Base legal y autorizaciones. Obtendrá y conservará prueba de las autorizaciones y comunicará finalidades y canales a los titulares.

iii. Calidad de datos. Suministrará información veraz, completa y actualizada; comunicará rectificaciones/actualizaciones oportunamente.

iv. Derechos de titulares. Tramitará consultas (10 días) y reclamos (15 días) hábiles; el ENCARGADO apoyará con evidencias y trazabilidad.

v. RNBD e incidentes. Registrará/actualizará las bases y flujos internacionales cuando aplique y realizará el reporte a la SIC de incidentes en ≤ 15 días hábiles, informando al ENCARGADO y requiriendo su soporte.

vi. Nube/transferencias y subencargados. Aprobará regiones de nube, flujos internacionales y subencargados, y comunicará restricciones o cambios que afecten el Tratamiento.

vii. Canales y acceso. Proveerá canales seguros y accesos necesarios (VPN/SFTP/portal), así como RPO/RTO y lineamientos técnicos aplicables.

viii. Supervisión y due diligence. Podrá auditar cumplimiento y solicitar evidencias (p. ej., informes ISO/SOC, pruebas de seguridad) y planes de acción.

ix. Cambios relevantes. Notificará al ENCARGADO cualquier cambio de finalidades, categorías de datos, bases, transferencias o normativa que afecte el Tratamiento.

CONFIDENCIALIDAD

Alcance y definición. Se considera Información Confidencial toda información relacionada con este Acuerdo (incluidos acuerdos, preacuerdos, correos, anexos, especificaciones técnicas, configuraciones, accesos y documentación), divulgada por cualquier medio, marcada o no como confidencial.

Cuando la Información Confidencial sea dato personal, aplican además las obligaciones específicas de protección de datos; en caso de conflicto, prevalece el estándar más estricto.

Uso limitado y necesidad de conocer. Cada Parte usará la Información Confidencial exclusivamente para ejecutar el Contrato y la revelará solo a su personal y asesores que necesiten conocerla, estén sujetos a confidencialidad y hayan sido autorizados. El ENCARGADO responde por sus dependientes y subencargados autorizados.

Medidas de resguardo. La Parte receptora protegerá la Información Confidencial con medidas técnicas, organizativas y jurídicas no inferiores a las que aplica a su propia información sensible y a las acordadas en el Anexo de Seguridad (incluyendo canales cifrados, control de acceso y registro de accesos).

Excepciones. No será Información Confidencial la que: (a) sea o llegue a ser pública sin infracción de la Parte receptora; (b) conste previamente en sus archivos sin deber de reserva; (c) sea legítimamente recibida de un tercero sin deber de confidencialidad; o (d) sea desarrollada de forma independiente sin usar la información de la Parte reveladora.

Divulgación requerida por ley. Si una autoridad exige divulgar Información Confidencial, la Parte receptora lo notificará previamente (cuando sea legalmente posible), limitará la divulgación a lo estrictamente requerido y conservará soporte de lo actuado.

No licencia y propiedad. Este Contrato no otorga licencias ni derechos de propiedad intelectual o sobre bases de datos, salvo lo estrictamente necesario para cumplir su objeto.

Plazo. Las obligaciones de confidencialidad rigen durante la vigencia del Contrato y por cinco (5) años posteriores a su terminación; respecto de secretos industriales y datos personales, la obligación pervive mientras conserven tal carácter o lo exija la ley.

Devolución/Eliminación. A la terminación o por requerimiento escrito, la Parte receptora devolverá o eliminará la Información Confidencial (incluidos respaldos) y emitirá certificación en un máximo de diez (10) días hábiles, salvo conservación legal; los datos permanecerán bloqueados mientras existan responsabilidades.

Remedios. El incumplimiento dará lugar a las acciones y resarcimientos previstos en la ley y en el Contrato, incluida la posibilidad de medidas cautelares para prevenir o cesar la divulgación o uso no autorizado, sin perjuicio de las obligaciones específicas sobre datos personales.

Comunicaciones públicas. Ninguna Parte realizará anuncios públicos sobre la relación contractual que revelen Información Confidencial sin autorización previa y escrita de la otra.

TERMINACIÓN DEL ACUERDO

El presente **ACUERDO DE CONFIDENCIALIDAD** terminará por las siguientes causas:

i. Por el incumplimiento total o parcial de una cualquiera de las partes de una cualesquiera de las obligaciones del presente Acuerdo. La terminación se producirá inmediatamente, una vez producido el hecho generador de incumplimiento.
ii. Por mutuo acuerdo entre las partes.
iii. Por ser declarada cualquiera de las Partes en estado judicial de suspensión de pagos, quiebra o concurso de acreedores y fuese demostrada una situación de insolvencia o cese de actividades, o se iniciase un proceso de liquidación o disolución.

EL RESPONSABLE podrá dar por terminado y de forma unilateral el presente acuerdo por las siguientes causas:

i. Por el incumplimiento total o parcial de las obligaciones establecidas en cabeza del **ENCARGADO.**
ii. Por negativas del **ENCARGADO** a brindar explicaciones técnicas y satisfactorias relacionadas con la ejecución del servicio contratado, cuando **EL RESPONSABLE** lo solicite, quien dejará constancia por escrito de tal negativa que servirá de prueba para determinar esa causal de terminación.
iii. Por decisión unilateral del **RESPONSABLE,** para lo cual dará un avisó con una antelación no inferior a un (1) día hábil al **ENCARGADO. PARÁGRAFO PRIMERO:** En caso de terminación del presente acuerdo, **EL ENCARDADO** deberá: Suspender todas las actividades encaminadas al Tratamiento de Datos Personales reguladas en este **ACUERDO DE CONFIDENCIALIDAD** o derivado del Contrato de prestación de servicios. Remitir de regreso y eliminar inmediatamente, según lo indicado por EL RESPONSABLE, toda la información de EL RESPONSABLE de la que tenga control, incluyendo, pero sin limitarse a los Datos Personales, y todas las copias de estos, que se encuentren en su posesión, custodia o control, salvo obligaciones legales de conservación o archivo de información. La terminación de este **ACUERDO DE CONFIDENCIALIDAD** se hará sin perjuicio de los derechos o compensaciones a que haya lugar o cualquier obligación o responsabilidad que se haya generado para cualquiera de las Partes, a la fecha efectiva de terminación.

CLÁUSULA DE SALVAGUARDA

Las cláusulas del presente ACUERDO son independientes y deben ser consideradas una a una, de tal forma que, si alguna de ellas pasara a ser inválida, ilegal o inejecutable en virtud de alguna norma jurídica, se considerará ineficaz en la medida que corresponda, pero en lo demás, este ACUERDO conservará su validez y eficacia en cuanto al resto del contenido, estipulaciones y obligaciones. Las Partes acuerdan sustituir la cláusula o cláusulas afectadas de invalidez, ilegalidad o imposibilidad de ejecutar por otra u otras que tengan los efectos económicos más parecidos a los de las sustituidas.

CESIÓN

Ninguna de las Partes podrá ceder este ACUERDO o cualquiera de los derechos u obligaciones contenidos en el mismo a un tercero sin el previo consentimiento escrito de la otra Parte.

LEGISLACIÓN APLICABLE

Para la resolución de todas las controversias o cuestiones relacionadas con el presente acuerdo, será de aplicación directa la legislación colombiana, específicamente el Ley 1581 de 2012 y normas reglamentarias, Código Civil, Código de Comercio y demás legislación vigente aplicable a las relaciones comerciales entre empresas, renunciando expresamente a cualquier otro tipo de legislación aplicable.

DELITOS CIBERNÉTICOS E INFORMÁTICOS (Título VII Bis C.P.)

1. **Cumplimiento y prohibición.** Las Partes, su personal y subencargados se abstendrán de realizar conductas tipificadas en el Título VII Bis del Código Penal Colombiano y normas concordantes, y adoptarán medidas razonables de prevención y control.
2. **Detección y aviso.** Ante indicios razonables de una conducta de esta naturaleza que afecte o pueda afectar la información o los sistemas de la otra Parte, la Parte que los detecte notificará en ≤ 48 horas, activará su plan de incidentes, preservará evidencias (logs, imágenes forenses, respaldos) y cooperará con investigaciones internas y de autoridad competente.
3. **Medidas preventivas.** Sin perjuicio de la presunción de inocencia, la Parte afectada podrá suspender de inmediato accesos, credenciales y sesiones, y realizar auditorías técnicas para contención y verificación; la otra Parte facilitará dichas actuaciones.
4. **Causal de terminación.** La comisión de cualquiera de los delitos del Título VII Bis, declarada mediante sentencia ejecutoriada, constituirá incumplimiento grave y causal de terminación con justa causa, sin perjuicio de las indemnizaciones a que haya lugar. Lo anterior no limita la adopción de medidas cautelares contractuales (p. ej., suspensión de servicios/accesos) durante la investigación.
5. **Responsabilidad.** La Parte incurra o cuyo personal/subencargados incurran en estas conductas responderá por perjuicios directos, costos razonables de contención/forense, sanciones y multas impuestas por autoridad, en la medida permitida por la ley.
6. **Coordinación con protección de datos.** Si el hecho constituye incidente de seguridad o afecta datos personales, se aplicarán además las obligaciones de la cláusula de gestión de incidentes y reporte a la autoridad previstas en este Contrato.

AUTORIZACIÓN DE USO DE DATOS PERSONALES.

LA JUNTA NACIONAL DE CALIFICACIÓN DE INVALIDEZ, será el responsable del tratamiento y, en tal virtud, podrá recolectar, usar, almacenar, circular y eliminar los datos personales **DEL ENCARGADO** para las siguientes finalidades:

Autorización expresa.

Con la firma de este documento, el Titular autoriza de manera libre, previa, expresa e informada a la JNCI para recolectar, usar, almacenar, circular y suprimir los datos personales que suministre o que sean recolectados directamente por JNCI en el marco de la relación contractual.

Finalidades del tratamiento.

Los datos se tratarán exclusivamente para:

1. Gestión administrativa y contractual del vínculo con el ENCARGADO (altas, certificaciones, coordinación operativa).
2. Comunicaciones operativas y de soporte técnico/administrativo relacionadas con la prestación del servicio.
3. Gestión de pagos, facturación y tesorería (validaciones bancarias y tributarias).

4. Cumplimiento de obligaciones legales, regulatorias y de auditoría; atención de requerimientos de autoridad.
5. Seguridad de la información y continuidad del negocio (controles de acceso a sistemas, trazabilidad).
6. Control de acceso y seguridad física en instalaciones de JNCI (incluida imagen captada por CCTV).
7. Gestión de PQR y ejercicio de derechos de protección de datos.

Datos sensibles.

Cuando sea necesario para las finalidades anteriores, el Titular autoriza el tratamiento de datos sensibles (p. ej., rasgos biométricos contenidos en el documento de identidad e imagen en CCTV) exclusivamente para control de acceso, seguridad y cumplimiento legal/contractual.

Encargados, subencargados y transferencias.

El Titular autoriza que sus datos se compartan con proveedores y subencargados que apoyen a JNCI en estas finalidades incluidos servicios en la nube, dentro o fuera de Colombia, bajo medidas de seguridad y conforme a la normativa aplicable.

Política y canales.

El tratamiento se realizará conforme a la Política de Tratamiento de Datos Personales de la JNCI, disponible en sus instalaciones y sitio web. Para acceder, actualizar, rectificar, suprimir o revocar la autorización, el Titular podrá escribir a protecciondatos@juntanacional.com o usar los canales de atención de la JNCI.

Vigencia y revocatoria.

Esta autorización rige desde su firma y durante la relación y los plazos legales de conservación. El Titular podrá revocar la autorización en cualquier momento, salvo cuando exista un deber legal o contractual que exija conservar la información.

Declaración sobre terceros.

Si el firmante entrega datos de otras personas, declara que les informó y que cuenta con su autorización o con la base legal correspondiente.

ENTRADA EN VIGOR Y DURACIÓN

La vigencia del presente ACUERDO inicia en la fecha de firma. No obstante, sus obligaciones aplican respecto de cada Dato Personal al que haya accedido EL ENCARGADO desde el inicio de las actividades asociadas al Servicio.

Las obligaciones de confidencialidad regirán durante el contrato y por cinco (5) años adicionales, o por el tiempo que la información conserve carácter confidencial; las obligaciones sobre datos personales se mantendrán mientras exista base legal de conservación y, en su defecto, hasta su supresión o bloqueo.

Parágrafo 1. Este ACUERDO es anexo obligatorio del Contrato de Consultoría suscrito a través de la plataforma SECOP II; servirá como marco de interpretación en lo no previsto por dicho contrato.
Parágrafo 2. La firma electrónica o digital confiere plena validez y fuerza probatoria conforme a la ley.

EL RESPONSABLE,

Firmado por:
Victor Hugo Trujillo Hurtado
2026/05/08 11:04:36:348

VÍCTOR HUGO TRUJILLO HURTADO
Representante legal
JUNTA NACIONAL DE CALIFICACIÓN DE INVALIDEZ

EL ENCARGADO,

EMILY VALERIA LADINO AGUILAR
Representante legal
UT NAFILEX DOC 2026

Anexo Técnico para proveedores de Alto Riesgo

Parte I: Acuerdo sobre Medidas Generales de Seguridad, SLA y Transferencias/Nube

Entre **EL RESPONSABLE** y **EL ENCARGADO** acuerdan lo siguiente:

Cláusula 1. Objeto. Este Anexo desarrolla las medidas técnicas, organizativas y jurídicas mínimas que EL ENCARGADO implementará para asegurar la confidencialidad, integridad, disponibilidad y resiliencia de la información y de los datos personales tratados por cuenta de EL RESPONSABLE, durante la vigencia del Contrato y, cuando aplique, con posterioridad a su terminación.

Cláusula 2. Gobierno y acceso. EL ENCARGADO administrará el acceso bajo estricta necesidad de conocer, con doble factor de autenticación (MFA), perfiles RBAC, altas y bajas de usuarios en un plazo máximo de veinticuatro (24) horas, y revisión trimestral de permisos. Las credenciales serán robustas, con rotación periódica y tiempos de expiración de sesión.
Cláusula 3. Cifrado y resguardo. La información se protegerá mediante cifrado en tránsito (protocolos vigentes) y en reposo (cifrado fuerte en bases y respaldos). La gestión de llaves será segregada y trazable.

Cláusula 4. Endpoints, redes y monitoreo. EL ENCARGADO mantendrá endurecimiento de equipos, EDR/antimalware, segmentación de red y controles perimetrales. Conservará registros (logs) de accesos administrativos, cambios y transferencias por un periodo mínimo de [6–12] meses, asegurando cadena de custodia.

Cláusula 5. Vulnerabilidades y parches. Existirá un proceso de gestión de vulnerabilidades y de parcheo regular, con escaneo continuo y al menos una prueba de penetración anual. Los plazos de remediación serán: críticas ≤ 72 horas; altas ≤ 7 días; medias ≤ 30 días.

Cláusula 6. Continuidad y respaldos. Los backups serán cifrados, con pruebas periódicas de restauración y RPO/RTO acordados con EL RESPONSABLE. Se llevará registro de ubicaciones, réplicas y restauraciones.
Cláusula 7. Intercambio seguro. Toda remisión de información o acceso remoto para soporte se realizará exclusivamente por VPN, SFTP o portales cifrados previamente aprobados por EL RESPONSABLE; se prohíbe el uso de canales no autorizados y la descarga a dispositivos personales.

Cláusula 8. Transferencias, transmisiones y nube. Cualquier transferencia o transmisión internacional de información asociada al Servicio procederá únicamente cuando el país de destino cuente con nivel adecuado de protección o existan garantías apropiadas, y, cuando corresponda, mediando la declaración de conformidad ante la autoridad competente. Requerirá autorización previa y escrita de EL RESPONSABLE. Las copias de seguridad y demás componentes en nube se alojarán únicamente en proveedores y regiones preaprobados por EL RESPONSABLE, con cifrado en tránsito y reposo, custodia segura de llaves, segregación lógica y control de acceso por privilegio mínimo. Se prohíbe la replicación, sincronización o tratamiento fuera de las regiones aprobadas y la descarga a dispositivos no autorizados. Todo subencargado de nube requerirá autorización previa y quedará sujeto a obligaciones no menos estrictas que las aquí pactadas. A la terminación, EL ENCARGADO devolverá o suprimirá respaldos y réplicas (incluidos metadatos) y emitirá certificación de borrado seguro dentro de diez (10) días hábiles; mientras subsistan obligaciones legales, los datos permanecerán bloqueados.

Cláusula 9. Incidentes (SLA). EL ENCARGADO notificará a EL RESPONSABLE sin dilación indebida y dentro de las veinticuatro (24) horas siguientes a la detección de un incidente que afecte datos personales o información del Servicio; remitirá informe técnico inicial dentro de setenta y dos (72) horas, y cooperará para el reporte a la autoridad competente dentro de los quince (15) días hábiles siguientes a la detección, así como para la remediación y las comunicaciones a titulares cuando corresponda.

Cláusula 10. Auditoría y verificación. EL RESPONSABLE podrá auditar, de forma remota o in situ y con preaviso razonable, el cumplimiento de este Anexo. EL ENCARGADO facilitará las evidencias necesarias (incluidos reportes ISO/SOC si existen) y ejecutará los planes de acción acordados.

Parte II: Anexo Técnico para Tratamientos con Datos Sensibles y Régimen de Penalidades Solidarias

De común acuerdo, las Partes estipulan que, cuando el Servicio involucre datos sensibles o tratamientos de alto riesgo, regirá este Anexo técnico, sin perjuicio de lo dispuesto en la parte I.

Cláusula 1. Activación y alcance. Este Anexo se activa cuando el tratamiento comprenda datos sensibles (v. gr., salud, biométricos —incluida imagen en CCTV o rasgos en documento de identidad—, u otras categorías especialmente protegidas) o suponga **alto riesgo** por volumen, criticidad, exposición internacional o naturaleza del proceso.

Cláusula 2. Evaluación y diseño de controles. Antes de iniciar el tratamiento, EL ENCARGADO realizará un Análisis de Impacto/Riesgo (PIA) específico y documentará controles reforzados. Toda modificación sustancial del proceso exigirá la actualización del PIA y, de ser el caso, nueva autorización de EL RESPONSABLE.

Cláusula 3. Minimización, entornos y extracción. El acceso a datos sensibles se limitará a lo estrictamente necesario, priorizando acceso controlado a los sistemas de EL RESPONSABLE. Queda prohibido utilizar datos sensibles reales en desarrollo o pruebas; se emplearán datos sintéticos o enmascarados. Se prohíbe la extracción y copia local de datos sensibles salvo instrucción escrita y bajo controles equivalentes a los productivos.

Cláusula 4. Accesos privilegiados y trazabilidad. Los accesos privilegiados serán MFA-obligatorios, con registro exhaustivo (usuario, fecha, caso, sistemas y campos accedidos) y, cuando aplique, grabación de la sesión. Se prohíbe la impresión o reproducción de datos sensibles.

Cláusula 5. Conservación y cierre. Los datos sensibles se conservarán por el tiempo mínimo necesario y legal. A la finalización del tratamiento, EL ENCARGADO suprimirá o devolverá la información y destruirá respaldos y metadatos asociados, emitiendo certificación dentro de diez (10) días hábiles; cuando exista obligación legal de conservar, los datos permanecerán bloqueados.

Cláusula 6. Subencargados y cadena internacional. Cualquier subencargado que intervenga en datos sensibles requerirá autorización previa y escrita de EL RESPONSABLE y quedará sujeto, por escrito, a obligaciones no menos estrictas que las de este Anexo, incluyendo ubicación/país de tratamiento, medidas de seguridad, auditorías y cooperación para incidentes y derechos de titulares.

Cláusula 7. SLA reforzado de incidentes. Ante un incidente que afecte datos sensibles, EL ENCARGADO avisará de inmediato y, en todo caso, dentro de las doce (12) horas siguientes a su detección, presentará informe técnico inicial en cuarenta y ocho (48) horas, y análisis de causa raíz y plan de remediación en diez (10) días. Propondrá la notificación a titulares cuando sea procedente y apoyará el reporte ante la autoridad.

Cláusula 8. Régimen de penalidades e indemnidad solidaria.

8.1. **Cláusula penal por incumplimientos materiales (datos sensibles).** La realización de cualquiera de las siguientes conductas: tratamiento sin instrucción, fuera de finalidad, subencargado no autorizado, transmisión/replicación fuera de región aprobada, no supresión oportuna al cierre, o retraso en el aviso de incidente más allá del SLA fijado, generará a cargo de EL ENCARGADO una cláusula penal equivalente al quince por ciento (15%) del valor mensual del contrato por cada evento, hasta un tope del cien por ciento (100%) del valor anual del contrato.

8.2. **Penalidad por incidente evitable con datos sensibles.** Si un incidente que afecte datos sensibles es atribuible a dolo o culpa de EL ENCARGADO o de sus subencargados, se causará, además, una penalidad del veinticinco por ciento (25%) del valor anual del contrato, lo que resulte mayor, sin perjuicio de la indemnización de perjuicios directos que haya lugar.

8.3. **Sanciones administrativas — asunción solidaria.** Si EL RESPONSABLE es sancionado por la autoridad competente por hechos imputables a EL ENCARGADO y/o sus subencargados, EL ENCARGADO asumirá y pagará solidariamente junto con el subencargado responsable las multas, sanciones, costas y gastos (incluidos honorarios periciales y de defensa) que deriven directamente de dicho incumplimiento, una vez exista decisión en firme, y reembolsará a EL RESPONSABLE cualquier suma que este hubiere pagado por tal concepto dentro de los quince (15) días siguientes al requerimiento escrito.

8.4. **Solidaridad en la cadena.** EL ENCARGADO responderá solidariamente frente a EL RESPONSABLE por los incumplimientos de sus subencargados vinculados al Servicio.

8.5. **Retención y compensación.** EL RESPONSABLE podrá retener pagos y compensar valores por penalidades, sanciones y perjuicios derivados del incumplimiento, conforme a la ley.

8.6. **Límites.** Los límites de responsabilidad que pudieran haberse pactado no aplicarán en casos de dolo o culpa grave, ni frente a violaciones de confidencialidad o de este Anexo técnico sobre datos sensibles.

Cláusula 9. Garantía de cumplimiento y manejo de información.

En caso de incumplimiento por parte del ENCARGADO de las obligaciones y disposiciones establecidas en el presente documento, se dará lugar a la activación de la garantía de cumplimiento del contrato, la cual se entenderá incorporada y vinculada al presente instrumento como parte integral del mismo.

Cláusula 10. Auditoría reforzada y evidencias. EL RESPONSABLE podrá efectuar auditorías extraordinarias ante incidentes o hallazgos críticos. EL ENCARGADO garantizará el acceso a registros, bitácoras, informes forenses y al personal involucrado, sin perjuicio de la reserva de secretos industriales, que no podrá invocarse para eludir verificaciones de cumplimiento.

Cláusula 11. Entrada en vigor. Este Anexo rige desde la suscripción de este acuerdo y mientras perdure el tratamiento de datos sensibles o de alto riesgo; al cierre, aplican las reglas de supresión certificada y bloqueo cuando exista conservación legal.

GLOSARIO

1. **Dato personal:** Información que identifica o hace identificable a una persona natural (p. ej., nombre, cédula, correo).
2. **Dato sensible:** Dato que afecta la intimidad o puede generar discriminación (salud, biométricos, orientación, etc.). (Véase Anexo 2, Cl.1).
3. **Titular:** Persona natural dueña del dato personal.
4. **Responsable del tratamiento:** Quien define finalidades y medios del tratamiento.
5. **Encargado del tratamiento:** Quien trata datos **por cuenta** del Responsable y según sus instrucciones.
6. **Subencargado:** Tercero contratado por el Encargado para apoyar el tratamiento. Debe estar autorizado y con obligaciones “flujo-down”. (Véase Anexo 1, Cl.8 y Anexo 2, Cl.6).
7. **Tratamiento:** Cualquier operación sobre datos: recolección, uso, almacenamiento, circulación, supresión, etc.
8. **Transmisión de datos:** Comunicación de datos del Responsable al Encargado para tratamiento por cuenta de aquel (dentro o fuera de Colombia). (Véase Anexo 1, Cl.8).
9. **Transferencia internacional:** Envío de datos a un **receptor Responsable** ubicado en otro país. (Véase Anexo 1, Cl.8).
10. **Nivel adecuado de protección:** Estándar exigido por la autoridad colombiana al país de destino; si no existe, se requieren garantías. (Véase Anexo 1, Cl.8).
11. **Declaración de conformidad:** Autorización de la SIC para ciertas transferencias a países sin nivel adecuado. (Véase Anexo 1, Cl.8).
12. **RNBD (Registro Nacional de Bases de Datos):** Registro/actualización de bases y reportes ante la SIC cuando aplique.
13. **SIC:** Superintendencia de Industria y Comercio; autoridad de protección de datos en Colombia. (Véase Anexo 1, Cl.9).
14. **Política de Tratamiento de Datos Personales:** Documento del Responsable con finalidades, medidas y canales para ejercer derechos. (Véase Autorización).
15. **Autorización (consentimiento):** Voluntad libre, previa, expresa e informada del Titular para tratar sus datos. (Véase Autorización).
16. **Pseudonimización:** Reemplazo de identificadores por códigos; permite reidentificar con llave separada. (Véase Anexo 2, Cl.3).
17. **Anonimización:** Transformación irreversible para que no sea posible identificar al Titular. (Véase Anexo 2, Cl.3).
18. **PIA (Privacy/Personal Data Impact Assessment):** Evaluación de impacto/riesgo del tratamiento. (Véase Anexo 2, Cl.2).
19. **MFA (Multi-Factor Authentication):** Autenticación con dos o más factores. (Véase Anexo 1, Cl.2).
20. **RBAC (Role-Based Access Control):** Control de acceso por roles y privilegio mínimo. (Véase Anexo 1, Cl.2).
21. **EDR (Endpoint Detection & Response):** Detección y respuesta a amenazas en equipos finales. (Véase Anexo 1, Cl.4).

22. **DLP (Data Loss Prevention):** Controles para prevenir fuga de información. (Véase Anexo 2, Cl.10).
23. **WAF (Web Application Firewall):** Filtro para proteger aplicaciones web. (Véase Anexo 1, Cl.4).
24. **DRP (Disaster Recovery Plan):** Plan de recuperación ante desastres. (Véase Anexo 1, Cl.6).
25. **RPO / RTO:** Objetivo de punto de recuperación (pérdida máxima de datos) / tiempo máximo de recuperación. (Véase Anexo 1, Cl.6).
26. **Logs (registros):** Bitácoras de accesos y cambios para auditoría/forense. (Véase Anexo 1, Cl.4).
27. **Accountability (responsabilidad demostrada):** Capacidad de **probar** cumplimiento con evidencias, auditorías y registros.
28. **Cláusula penal:** Suma pre-pactada por incumplimiento contractual. (Véase Anexo 2, Cl.8.1).
29. **Responsabilidad solidaria:** Varios obligados responden **todos** por el total frente al acreedor. (Véase Anexo 2, Cl.8.3–8.4).
30. **Bloqueo de datos:** Conservación sin uso activo por obligación legal o mientras existan responsabilidades. (Véase Anexo 1, Cl.8 y Cl.6).
31. **Dato biométrico:** Rasgos físicos o conductuales que identifican a una persona (p. ej., huella, rostro/imagen). (Véase Anexo 2, Cl.1).

Firmado por:
Victor Hugo Trujillo Hurtado
2026/05/08 08:23:42:511

CONTRATANTE **VÍCTOR HUGO TRUJILLO HURTADO** **Representante Legal** **Junta Nacional Calificación de Invalidez**	**CONTRATISTA** **EMILY VALERIA LADINO AGUILAR** **Representante Legal** **UT NAFILEX DOC 2026**