

## CONDICIONES DE PRIVACIDAD Y SEGURIDAD PARA PROVEEDORES

Estas Condiciones de Privacidad y Seguridad para Proveedores establecen los derechos y las obligaciones de Kyndryl y del Proveedor en materia de gestión, seguridad y asuntos relacionados con los datos (las "**Condiciones**"). Las Condiciones se incorporan y forman parte del Acuerdo de Relación con Proveedores (o acuerdo equivalente) entre las partes, incluidas las Declaraciones de Trabajo, las Autorizaciones de Trabajo u otros documentos entre las empresas que hagan referencia a ellos (los "**Documentos de Transacción**").

Estas Condiciones consisten en:

- Este documento,
- El Suplemento de Detalles de Procesamiento adjunto al presente documento describe las actividades de procesamiento de datos del Proveedor como la aplicación de estas Condiciones (para cualquier Documento de Transacción celebrado después de la aplicación de estas Condiciones, se deberá adjuntar un Suplemento de Detalles de Procesamiento separado para cada Documento de Transacción, documentando las actividades de procesamiento del Proveedor específicas a ese documento), y
- Las Cláusulas Contractuales Tipo de la UE, el Apéndice sobre la Transferencia Internacional de Datos del Reino Unido y la Evaluación de Impacto de la Transferencia, que se encuentran en <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.

Las presentes Condiciones prevalecerán en caso de conflicto entre las disposiciones de este documento, el Acuerdo de Relación con Proveedores, un acuerdo equivalente o el Documento de Transacción, incluidos los acuerdos de procesamiento de datos. Si existe un conflicto entre estas Condiciones y las disposiciones acordadas mutuamente entre el Proveedor y Kyndryl para un Cliente de Kyndryl, prevalecerán las disposiciones acordadas mutuamente para el Cliente de Kyndryl.

Las palabras en mayúscula tienen el significado que se indica en el Artículo V de estas Condiciones, en otra parte de estas Condiciones, o en el Documento de Transacción o el acuerdo base asociado entre las partes.

### Article I. GESTIÓN DE DATOS E IA

- 1.1. **Cumplimiento de las leyes.** El Proveedor cumplirá con toda la legislación aplicable a los Servicios y Entregables, incluida la legislación relacionada con la protección de datos, la ciberseguridad y los Sistemas de IA. El Proveedor notificará de inmediato a Kyndryl (y en cualquier caso en los plazos requeridos por la ley y que brinden a Kyndryl la oportunidad de cumplir con sus propias obligaciones legales), si el Proveedor determina que ya no puede cumplir con sus obligaciones legales.
- 1.2. **Uso de Datos.** El proveedor no deberá:
  - (a) utilizar los Datos de Kyndryl en cualquier forma, incluso los datos agregados, anónimos o de otro tipo, para cualquier propósito distinto que no sea el de proporcionar Servicios y Entregables (a modo de ejemplo, el Proveedor no está autorizado a utilizar o reutilizar los Datos de Kyndryl para la evaluación de la eficacia o los medios para mejorar las ofertas del Proveedor que no sean los Servicios o Entregables, para la investigación y desarrollo para crear nuevas ofertas o para la generación de informes relacionados con las ofertas del Proveedor)
  - (b) Vender o Compartir los Datos de Kyndryl; o
  - (c) intentar volver a identificar cualquier información que pueda ser utilizada razonablemente para deducir información sobre o que de otro modo esté vinculada, a un Interesado.
- 1.3. **Tecnologías de Seguimiento Web.** Si el Proveedor o sus Subcontratistas, en la entrega de los Servicios o los Entregables, recopila información mediante tecnologías de seguimiento web (incluido HTML5, almacenamiento local, etiquetas o tokens de terceros y balizas web), dichos datos se considerarán Datos de Kyndryl y el Proveedor deberá cumplir con sus obligaciones con respecto a los Datos de Kyndryl según estas Condiciones.
- 1.4. **No divulgación.** El Proveedor no divulgará los Datos de Kyndryl a ningún tercero, salvo a los Subprocesadores aprobados de conformidad con la Sección 2.5 o a los Subcontratistas aprobados de conformidad con el Acuerdo.

- 1.5. **Acceso Gubernamental.** Si un gobierno, incluido cualquier regulador, exige acceso a los Datos de Kyndryl (por ejemplo, si el gobierno de los EE. UU. dicta una orden de seguridad nacional que afecta al Proveedor para obtener los Datos de Kyndryl), o si la ley requiere la revelación de los Datos de Kyndryl, el Proveedor notificará de inmediato a Kyndryl por escrito dicha demanda o requisito y brindará a Kyndryl la oportunidad razonable de impugnar la divulgación, a menos que la legislación lo prohíba. Si la legislación prohíbe la notificación, el Proveedor adoptará las medidas que razonablemente considere para impugnar la prohibición y la revelación de los Datos de Kyndryl mediante acciones judiciales u otros medios.
- 1.6. **Confidencialidad.** El Proveedor garantiza a Kyndryl que: (a) solo los empleados que necesiten acceso a los Datos de Kyndryl para prestar Servicios o Entregables tendrán ese acceso, y solo en la medida necesaria; y (b) sus empleados tienen obligaciones vinculantes de confidencialidad en virtud de las cuales solo pueden usar y divulgar los Datos de Kyndryl según lo permitido en estas Condiciones.
- 1.7. **Devolución o eliminación de Datos de Kyndryl.** El Proveedor, a elección de Kyndryl, eliminará o devolverá los Datos de Kyndryl a Kyndryl a su costa y al terminar o vencer el Documento de Transacción, o con anterioridad a petición de Kyndryl. Si Kyndryl requiere la eliminación, el Proveedor, de acuerdo con NIST SP 800-88 rev.1, hará que los datos sean ilegibles y no puedan reensamblarse o reconstruirse, y certificará la eliminación a Kyndryl, a petición. Si Kyndryl requiere la devolución de los Datos de Kyndryl, el Proveedor lo hará en un formato comúnmente utilizado según el programa y las instrucciones razonables de Kyndryl.
- 1.8. **Sistemas de IA**
- (a) El Proveedor no utilizará los Sistemas de IA en la entrega de los Servicios o un Entregable ni incluirá los Sistemas de IA en un Entregable, sin la autorización previa de Kyndryl en un Documento de Transacción o el Acuerdo. Al solicitar la autorización de Kyndryl, el Proveedor proporcionará a Kyndryl por escrito toda la información necesaria para evaluar el uso que hace el Proveedor de los Sistemas de IA (por ejemplo, flujos de datos, modelos de lenguaje usados, separación de datos).
  - (b) El Proveedor declara y garantiza que: (i) la aportación proporcionada por Kyndryl (incluida la aportación proporcionada por los empleados o cualquier tercero bajo un Documento de Transacción) y el resultado será clasificado como Materiales de Kyndryl, (ii) el Proveedor no utilizará los Materiales de Kyndryl para entrenar o ajustar el modelo base u otros elementos de los Sistemas de IA, (iii) el Proveedor no almacenará los Materiales de Kyndryl más tiempo del necesario para prestar los Servicios, (iv) los Sistemas de IA (incluidos los resultados y los datos de entrenamiento) se clasificarán como parte de los Servicios y (v) en la medida que la legislación lo permita, el Proveedor por la presente asigna todos sus derechos, títulos e intereses en y hacia los resultados de los Sistemas de IA a Kyndryl.
  - (c) El Proveedor deberá implementar y mantener un programa documentado de gestión y gestión de riesgos para los Sistemas de IA que identifique, pruebe, supervise y mitigue razonable y apropiadamente los riesgos conocidos y previsibles, incluidos, entre otros, los riesgos relacionados con la ética, los sesgos, la seguridad y la protección asociados con o derivados de los Sistemas de IA. A petición, el Proveedor compartirá una copia de su programa de gestión y gestión de riesgos para los Sistemas de IA. El Proveedor notificará de inmediato a Kyndryl por escrito cualquier riesgo que haya ocurrido o cualquier riesgo material que haya sido identificado de conformidad con la disposición de notificación acordada en el Documento de Transacción enviando una copia a [ailegalteam@kyndryl.com](mailto:ailegalteam@kyndryl.com).

## Article II. PRIVACIDAD

- 2.1. **Información de Contacto Comercial.** Kyndryl y el Proveedor pueden procesar la Información de Contacto de Negocios de cada uno de conformidad con las leyes de protección de datos aplicables como Controladores independientes dondequiera que realicen negocios para prestar y recibir los Entregables y los Servicios. Las partes no actúan como Controladores conjuntos en relación con la Información de Contacto de Negocios de cada una. Si cualquiera de las partes comunica a la otra parte sobre cualquier solicitud de un Interesado con respecto a la Información de Contacto de Negocios de la otra parte, la otra parte será responsable de abordar dichas solicitudes directamente con el Interesado. Cada una de las partes ha implementado las medidas técnicas y organizativas apropiadas para proteger la Información de Contacto de Negocios de la otra parte. Para mayor claridad, la Sección 3.12 (Incidentes de Seguridad) se aplica a la Información de Contacto Comercial.

2.2. **Proveedor como Procesador.** Kyndryl designa al Proveedor como Procesador de los Datos Personales de Kyndryl con el único propósito de proporcionar los Entregables y los Servicios de conformidad con las instrucciones de Kyndryl, incluidas las contenidas en estas Condiciones, el Acuerdo y cualquier Documento de Transacción relacionado. El Proveedor es un Procesador de los Datos Personales de Kyndryl. Si el Proveedor no actúa de conformidad con las instrucciones de Kyndryl para que Kyndryl cumpla con las leyes de protección de datos aplicables, Kyndryl podrá rescindir la parte afectada de los Servicios mediante una notificación por escrito. Si el Proveedor considera que una instrucción infringe una ley de protección de datos, el Proveedor lo notificará a Kyndryl de inmediato y dentro de cualquier plazo que requiera la legislación pertinente.

2.3. **Medidas Técnicas y Organizativas.** El Proveedor implementará y mantendrá las medidas técnicas y organizativas apropiadas, incluidas las medidas de seguridad el Artículo III a continuación, para garantizar el nivel de seguridad adecuado al riesgo asociado con la entrega de los Servicios y los Entregables.

#### 2.4. **Solicitudes y Derechos de los Interesados**

- (a) El Proveedor notificará a Kyndryl de inmediato (según un calendario que permita a Kyndryl y a cualquier Otro Controlador cumplir sus obligaciones legales) sobre cualquier solicitud de un Interesado para ejercer cualquier derecho del Interesado (por ejemplo, rectificación, eliminación o bloqueo de datos) con respecto a los Datos personales de Kyndryl. El Proveedor también puede dar instrucciones de inmediato a un Interesado que efectúe una petición a Kyndryl. El Proveedor no responderá a las solicitudes de los Interesados a menos que lo exija la legislación o que Kyndryl lo requiera por escrito.
- (b) Si Kyndryl está obligado a proporcionar información sobre los Datos Personales de Kyndryl a Otros Controladores u otros terceros (por ejemplo, Interesados o reguladores), el Proveedor ayudará a Kyndryl proporcionando información y llevando a cabo otras acciones razonables que Kyndryl solicite, según un calendario que permita a Kyndryl responder oportunamente a dichos Otros Responsables del Procesamiento de Datos o terceros.

#### 2.5. **Subprocesadores**

- (a) Kyndryl autoriza al Proveedor a contratar a los Subprocesadores enumerados en los respectivos Suplementos de Detalles de Procesamiento. El Proveedor también podrá contratar Subprocesadores adicionales o sustitutos, o ampliar el alcance del Procesamiento realizado por un Subprocesador existente, sujeto a lo siguiente:
  - (i) El Proveedor notificará por escrito a Kyndryl con antelación antes de proceder con cualquiera de dichos cambios.
  - (ii) Kyndryl podrá oponerse, por motivos razonables, a cualquier Subprocesador nuevo o sustituto, o a cualquier ampliación del alcance del Procesamiento, y las partes colaborarán de buena fe para abordar dicha objeción.
  - (iii) Sujeto al derecho de Kyndryl de objetar en cualquier momento, el Proveedor puede proceder con el cambio si Kyndryl no ha presentado una objeción dentro de los 30 días posteriores a la recepción de la notificación por escrito del Proveedor.
- (b) El Proveedor impondrá las obligaciones de protección de datos, seguridad y certificación establecidas en estas Condiciones a cada Subprocesador aprobado antes de que un Subprocesador procese los Datos Personales de Kyndryl. El Proveedor es plenamente responsable ante Kyndryl por el cumplimiento de las obligaciones de cada Subprocesador.

#### 2.6. **Procesamiento de Datos Transfronterizo**

- (a) El Proveedor no transferirá ni divulgará (incluido mediante acceso remoto) ningún Dato Personal de Kyndryl internacionalmente, salvo a Subprocesadores aprobados de conformidad con la Sección 2.5. Si Kyndryl aprueba la transferencia transfronteriza de los Datos Personales de Kyndryl, las partes cooperarán para cumplir con las leyes de protección de datos aplicables. Si dichas leyes exigen unas CCT, el Proveedor concertará de inmediato unas CCT tal y como se define más adelante.
- (b) **Espacio Económico Europeo**
  - (i) Si Kyndryl transfiere los Datos Personales sujetos al Reglamento General de Protección de Datos (2016/679) fuera del Espacio Económico Europeo a un Proveedor no situado en un País Adecuado, el Proveedor por la presente suscribe las Cláusulas Contractuales Tipo de la UE (Decisión de la Comisión

- 2021/914), firmadas previamente por Kyndryl y ubicadas en <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms> ("CCT de la UE").
- (ii) En caso de que Kyndryl desaparezca de hecho, deje de existir legalmente o se vuelva insolvente, los Otros Controladores tendrán el derecho de rescindir el Acuerdo y ordenar al Proveedor que borre o devuelva los Datos Personales de Kyndryl.
  - (iii) La evaluación de Kyndryl sobre las transferencias de Datos Personales a los Proveedores según lo exigen las CCT de la UE se publica para que el Proveedor la revise en <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.
  - (iv) El Proveedor proporcionará suficientes detalles de cada Subprocesador en los Suplementos de Detalles de Procesamiento y avisos para satisfacer sus obligaciones como importador de datos en virtud de la cláusula 14(c) de las Cláusulas Contractuales Tipo de la UE, incluyendo el nombre, las ubicaciones de procesamiento y las actividades de procesamiento del Subprocesador.
  - (v) El Proveedor actuará como Exportador de Datos y suscribirá las CCT de la UE u otro mecanismo de transferencia apropiado con cada Subprocesador aprobado no situado en un País adecuado.
- (c) **Reino Unido.** Si los Datos Personales de Kyndryl regulados por la Ley de Protección de Datos del Reino Unido (2018) se transfieren fuera del Reino Unido a un País no Adecuado, el Proveedor, por la presente, suscribe el Apéndice del Reino Unido sobre Transferencia Internacional de Datos (UK International Data Transfer Addendum), firmado previamente por Kyndryl y disponible en <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.
- (d) **Suiza.** Si los Datos Personales de Kyndryl sujetos a la Ley Federal Suiza de Protección de Datos ("FADP") se transfieren fuera de Suiza a un País no Adecuado, el Proveedor suscribe por la presente las CCT de la UE, con sujeción a las siguientes modificaciones:
- (i) las referencias al RGPD también incluirán la referencia a las disposiciones equivalentes de la FADP;
  - (ii) la Comisión Federal de Información y Protección de Datos de Suiza es la autoridad supervisora exclusiva de conformidad con la Cláusula 13 y el Anexo I.C de las CCT de la UE;
  - (iii) la ley aplicable de acuerdo con la Cláusula 17 de las CCT de la UE será la ley suiza en caso de que la transferencia de datos esté sujeta exclusivamente a la FADP; y
  - (iv) el término "estado miembro" no debe interpretarse de manera que excluya a los interesados en Suiza de la posibilidad de demandar sus derechos en su lugar de residencia habitual (Suiza) de conformidad con la Cláusula 18 de las CCT de la UE.
- (e) **Brasil.** Si Kyndryl transfiere Datos Personales sujetos a la Lei Geral de Proteção de Dados (LGPD) fuera de Brasil al Proveedor, que no esté establecido en un País Adecuado, el Proveedor, por la presente, suscribe el Anexo II de la Resolução CD/ANPD nº 19/2024 (en adelante, las "Cláusulas Contractuales Tipo de Brasil" o las "CCE de Brasil"), firmado previamente por Kyndryl y disponible en <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms> ("CCE de Brasil").
- (f) **Otros países.** Si una transferencia de Datos Personales de Kyndryl está sujeta a las leyes de protección de datos de un país donde las CCT locales no han sido publicadas por la Autoridad Supervisora (como la Ley de Protección de Datos de Perú, la Ley de Protección de Datos de Sudáfrica) o la Autoridad Supervisora ha aprobado el uso de las cláusulas contractuales tipo de la UE como salvaguarda suficiente para la transferencia transfronteriza (por ejemplo, la Ley de Protección de Datos de Argentina), las CCT de la UE regirán dicha transferencia con sujeción a las siguientes modificaciones:
- (i) las referencias al RGPD también incluirán la referencia a las disposiciones equivalentes de la legislación local sobre protección de datos;
  - (ii) la Autoridad Supervisora local es la autoridad de supervisión exclusiva de conformidad con la Cláusula 13 y el Anexo I.C de las CCT de la UE;
  - (iii) la legislación aplicable de conformidad con la Cláusula 17 de las CCT de la UE será la ley local de protección de datos; y
  - (iv) el término "estado miembro" no debe interpretarse de manera que excluya a los interesados en el país de la posibilidad de exigir sus derechos en su lugar de residencia habitual de conformidad con la Cláusula 18 de las CCT de la UE.

## 2.7. Asistencia y Registros

- (a) Teniendo en cuenta la naturaleza del Procesamiento, el Proveedor ayudará a Kyndryl mediante la adopción de Medidas Técnicas y Organizativas ("TOM") adecuadas a cumplir las obligaciones asociadas con las solicitudes y los derechos del Interesado. El Proveedor también ayudará a Kyndryl a garantizar el cumplimiento de las obligaciones relacionadas con la seguridad del Procesamiento, la notificación y

comunicación de un Incidente de Seguridad y la creación de evaluaciones de impacto en la protección de datos, incluida la consulta previa con el regulador responsable, si es necesario, teniendo en cuenta la información disponible para el Proveedor.

- (b) El Proveedor mantendrá un registro actualizado del nombre y los detalles de contacto de cada Subprocesador, incluyendo el delegado de protección de datos y representante del Subprocesador. Previa solicitud, el Proveedor proporcionará este registro a Kyndryl conforme a un calendario que permita a Kyndryl responder oportunamente a cualquier demanda de un Cliente u otro tercero.

## 2.8. Términos obligatorios del país

### (a) **Japón**

- i) Para la Información de Contacto Comercial de los Interesados ubicados en Japón, el Proveedor cumplirá con las disposiciones de estas Condiciones, aplicables al Proveedor como Procesador.
- ii) La definición de "Incidente de Seguridad" en estas Condiciones se modifica por la presente para incluir las filtraciones razonablemente sospechosas de Datos Personales de Kyndryl relacionados con los Interesados ubicados en Japón.
- iii) El Proveedor garantiza que no tiene motivos para creer que las leyes y prácticas de cualquier país donde el Proveedor o sus Subprocesadores procesarán Datos Personales de Kyndryl le impidan cumplir con sus obligaciones bajo estas Condiciones. El Proveedor notificará a Kyndryl si, después de haber aceptado las Condiciones y durante la duración de estas, el Proveedor tiene motivos para creer que no puede cumplir con su obligación bajo las Condiciones. En cuyo caso, las partes cooperarán de buena fe para identificar las medidas apropiadas que se deben adoptar para abordar la situación. Si no se pueden implementar medidas adecuadas, Kyndryl evaluará si suspender la transferencia de Datos Personales de Kyndryl.

- (b) **California.** Cuando el Proveedor, como Procesador, Procese los Datos Personales de Kyndryl de los Interesados ubicados en el Estado de California, (i) Kyndryl divulgará los Datos Personales de Kyndryl al Proveedor solo para los fines comerciales específicos y limitados seleccionados en el Suplemento de Detalles del Procesamiento, (ii) Kyndryl podrá, previa notificación, adoptar medidas adecuadas y razonables para detener el Procesamiento no autorizado o garantizar que el Procesamiento del Proveedor sea coherente con las obligaciones de Kyndryl bajo las leyes de protección de datos aplicables y (iii) el Proveedor no podrá conservar, utilizar ni divulgar los Datos Personales de Kyndryl fuera de la relación comercial directa entre este y Kyndryl.

### (c) **Canadá.**

- i) En relación con la Información de Contacto Comercial (BCI) de los Titulares de Datos ubicados en Canadá, el Proveedor cumplirá las disposiciones de estos Términos aplicables al Proveedor en su calidad de Procesador, en la medida en que dicha información sea considerada Datos Personales.
- ii) Para mayor claridad, las referencias a las leyes de protección de datos aplicables incluyen, sin limitación, todas las pautas y buenas prácticas legalmente vinculantes publicadas por una Autoridad de Supervisión en Canadá que tenga jurisdicción, según sean modificadas, reemplazadas o sustituidas.
- iii) El Proveedor no utilizará los Datos de Kyndryl para crear una base de datos de características biométricas o mediciones con fines de identificación personal.
- iv) El Proveedor llevará a cabo cualquier evaluación de impacto sobre la privacidad o evaluación de impacto sobre la transferencia que sea requerida por las leyes de protección de datos de Canadá, proporcionará una copia de dichas evaluaciones previa solicitud y notificará a Kyndryl sin demora indebida sobre cualquier medida complementaria que deba aplicarse.
- v) En caso de que Kyndryl no esté de acuerdo con los resultados de las evaluaciones del Proveedor o con cualquier medida complementaria, Kyndryl y el Proveedor trabajarán juntos para encontrar una solución viable. En caso de que las Partes no puedan llegar a un acuerdo sobre una solución viable, Kyndryl se reserva el derecho de suspender o dar por terminados los servicios del Proveedor en cuestión, sin compensación.
- vi) El Proveedor asistirá a Kyndryl proporcionando la información adicional que se solicite razonablemente para que Kyndryl realice su propia evaluación, conforme a las leyes de protección de datos aplicables de Canadá, sobre si los Términos proporcionan una protección adecuada.

## Article III. **SEGURIDAD GENERAL**

### 3.1. Políticas de Seguridad

- (a) **Políticas.** Las políticas de seguridad de la información del Proveedor estarán documentadas, aprobadas por la alta gerencia del Proveedor y serán coherentes con las Prácticas Estándar de la Industria, como las del Instituto Nacional de Estándares y Tecnología (NIST) y/o la Organización Internacional de Normalización (ISO). Las políticas de seguridad de la información del Proveedor serán revisadas y evaluadas por el Proveedor al menos una vez al año, y oportunamente después de cualquier cambio sustancial que se realice en dichas políticas, para confirmar su aplicabilidad y eficacia continuas. El Proveedor no realizará cambios a las políticas que puedan degradar la seguridad del Proveedor en relación con los Materiales de Kyndryl, los Entregables o los Servicios.
- (b) **Pruebas.** El Proveedor mantendrá un proceso para poner a prueba periódicamente la eficacia de sus medidas técnicas y organizativas para garantizar la seguridad de los Materiales de Kyndryl, los Entregables y los Servicios.
- (c) **Gestión de riesgos.** El Proveedor realizará evaluaciones de riesgos de seguridad de la información apropiadas como parte de un programa continuo gestión de riesgos con los siguientes objetivos: (i) identificar los riesgos de seguridad de la información relacionados con los Materiales de Kyndryl, los Entregables y los Servicios; (ii) evaluar el impacto de dichos riesgos; y (iii) cuando se identifiquen o justifiquen estrategias de reducción o mitigación de riesgos, implementar medidas para mitigar y gestionar eficazmente dichos riesgos reconociendo que el panorama de amenazas cambia constantemente.

### 3.2. Seguridad del personal

- (a) **Capacitación en seguridad.** El Proveedor brindará concientización, educación y capacitación adecuadas sobre seguridad y privacidad al menos una vez al año a todo su Personal que tenga acceso o la capacidad de acceder a los Materiales de Kyndryl, los Entregables o los Servicios.
- (b) **Verificación de Antecedentes.** El Proveedor actualizará y seguirá sus requisitos obligatorios y estándar de verificación de empleabilidad en las nuevas contrataciones y ampliará tales requisitos a todo el Personal del Proveedor y al Personal de las filiales controladas por el Proveedor. Dichos requisitos incluirán comprobaciones de antecedentes penales, según lo permitido por la legislación vigente, la validación de la prueba de identidad y las comprobaciones adicionales que el Proveedor estime oportunas. El Proveedor repetirá y revalidará estos requisitos periódicamente, según considere necesario.

### 3.3. Gestión de Activos

- (a) **Inventario de Activos.** El Proveedor mantendrá un inventario de activos de todos los equipos en los que se almacenan Materiales de Kyndryl. El Proveedor restringirá el acceso a dichos equipos únicamente al Personal autorizado del Proveedor. El Proveedor evitará el acceso no autorizado a los Materiales de Kyndryl, así como su copia, modificación o eliminación no autorizadas. El Proveedor mantendrá medidas para evitar el acceso, la copia, la modificación o la eliminación no autorizados de los Materiales de Kyndryl.
- (b) **Seguridad de los Componentes de Software.** El Proveedor se compromete a inventariar adecuadamente todos los componentes de software (incluido el software de código abierto) utilizados en la prestación de los Servicios y el desarrollo y suministro de los Entregables. El Proveedor evaluará si dichos componentes de software tienen defectos de seguridad y/o vulnerabilidades que podrían llevar a la divulgación o acceso no autorizado a los Materiales de Kyndryl, los Entregables o los Servicios. El Proveedor realizará dicha evaluación antes de la entrega o de brindar acceso a Kyndryl a los Servicios y Entregables y de manera continua posteriormente durante el plazo del Documento de Transacción. El Proveedor se compromete a solucionar oportunamente cualquier defecto de seguridad o vulnerabilidad en cualquier componente de software del que tenga conocimiento. El Proveedor responderá con prontitud a cualquier consulta de Kyndryl relacionada con si el Proveedor conoce algún defecto de seguridad o vulnerabilidad en dicho componente de software y/o si ha sido solucionados por el Proveedor.

- 3.4. **Política de Control de Acceso.** El Proveedor mantendrá una política adecuada de control de acceso basado en roles y medidas técnicas adecuadas de control de acceso, coherentes con las prácticas estándar de la industria, para restringir el acceso a los Materiales de Kyndryl y a los activos del Proveedor utilizados para prestar los Servicios únicamente al Personal autorizado del Proveedor, y para limitar dicho acceso al nivel mínimo necesario para prestar y brindar soporte a los Servicios y Entregables. Dicho acceso será registrado conforme a los requisitos establecidos en la Sección 3.10(f).

### 3.5. Autorización

- (a) El Proveedor mantendrá procedimientos de creación y eliminación de cuentas de usuario para otorgar y revocar rápidamente (y en cualquier caso dentro de las veinticuatro (24) horas) el acceso a todos los Materiales de Kyndryl y a todas las aplicaciones y activos internos del Proveedor utilizados en la prestación de los Servicios y Entregables. El Proveedor asignará una autoridad apropiada para aprobar la creación y revocación de la cuentas de usuario o niveles elevados o reducidos de acceso para cuentas existentes, incluso para la terminación del empleo, contrato, compromiso u otro acuerdo de un miembro del Personal con el Proveedor o un cambio de rol si dicho miembro del Personal ya no necesita dichos derechos de acceso.
- (b) El Proveedor mantendrá y actualizará registros del miembro del Personal del Proveedor que esté autorizado a acceder a los sistemas y activos en los que se almacenan, o desde los cuales se puede acceder a los Materiales de Kyndryl y los Entregables o que se utilizan para proporcionar los Servicios y revisará dichos registros al menos trimestralmente. Al Personal administrativo y de soporte técnico solo se le permitirá tener acceso a dichos sistemas, Materiales de Kyndryl y Entregables cuando sea necesario y siempre que dicho Personal cumpla con las medidas técnicas y organizativas aplicables del Proveedor.
- (c) El Proveedor garantizará que las cuentas de usuario que tengan acceso a dichos sistemas y activos sean únicas y estén restringidas por contraseñas y que las cuentas de usuario no se compartan.

### 3.6. Autenticación

- (a) El Proveedor supervisará los intentos repetidos de acceso a los sistemas y activos de información.
- (b) El Proveedor mantendrá prácticas de protección de contraseñas que sean consistentes con las Prácticas Estándar de la Industria y estén diseñadas para mantener la confidencialidad e integridad de las contraseñas generadas, asignadas, distribuidas y almacenadas en cualquier forma. El Proveedor generará o requerirá que el usuario cree y utilice una contraseña o frase de contraseña compleja generada aleatoriamente o alternativas adecuadas, como certificados digitales, tarjetas o tokens de hardware o biometría.
- (c) El Proveedor utilizará autenticación multifactor, incluso para el acceso administrativo al dominio y al portal en la nube. La autenticación multifactor puede incluir técnicas como el uso de certificados criptográficos, tokens de contraseña de un solo uso (OTP) o biometría.

### 3.7. Criptografía

- (a) **Política.** El Proveedor implementará y mantendrá políticas y estándares criptográficos consistentes con las Prácticas Estándar de la Industria para proteger los Materiales de Kyndryl, incluyendo, cuando corresponda, la seudonimización y el cifrado.
- (b) **Cifrado.** El Proveedor deberá cifrar los Materiales de Kyndryl en tránsito y en reposo. Los algoritmos de cifrado protegerán los datos a niveles de seguridad consistentes con las Prácticas Estándar de la Industria (como NIST SP 800-131a) y utilizarán funciones hash reconocidas por la industria, que serán al menos tan protectoras como el cifrado estándar de cifrado avanzado de 256 bits (AES 256) en reposo y TLS v1.2 en tránsito. El Proveedor mantendrá y seguirá políticas y prácticas de gestión de claves coherentes con las Prácticas Estándar de la Industria que definen los requisitos de clave de cifrado, seguridad, rotación y ciclo de vida, incluida la creación, distribución, revocación, archivo y destrucción.

### 3.8. Seguridad Física y Ambiental

- (a) **Acceso a Instalaciones.** El Proveedor limitará el acceso a las Instalaciones a su Personal autorizado.
- (b) **Protección contra Interrupciones.** El Proveedor realizará esfuerzos razonables para proteger dichos sistemas y activos contra fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.
- (c) **Eliminación Segura o Reutilización de Equipos.** El Proveedor se asegurará de que todos los Materiales de Kyndryl se hayan eliminado o sobrescrito de forma segura de los equipos que contienen medios de almacenamiento utilizando procesos consistentes con las Prácticas Estándar de la Industria antes de la eliminación o reutilización de dichos equipos.

### 3.9. Seguridad de Operaciones

- (a) **Política de Operaciones.** El Proveedor mantendrá procedimientos operativos y de seguridad adecuados y dichos procedimientos estarán disponibles para todo el Personal que los requiera.
- (b) **Protecciones contra Malware.** El Proveedor implementará soluciones antivirus y de gestión de puntos de conexión para mantener controles antimalware para proteger dichos sistemas y activos de software malicioso, incluido el software malicioso que se origina en redes públicas.

- (c) **Gestión de Configuración.** El Proveedor adoptará políticas que regulen la instalación de software y utilidades por parte del Personal.
- (d) **Gestión del Cambio.** El Proveedor mantendrá e implementará procedimientos para garantizar que solo se implementarán versiones aprobadas y seguras del código, las configuraciones, los sistemas y las aplicaciones en los entornos de producción.
- (e) **Separación Lógica.** El Proveedor mantendrá un aislamiento adecuado de sus entornos productivos y no productivos u otros entornos y, si los Materiales de Kyndryl ya existen en un entorno no productivo o se transfieren posteriormente a un entorno no productivo (por ejemplo, para reproducir un error), el Proveedor se asegurará de que las protecciones de seguridad y privacidad en el entorno no productivo sean equivalentes a las del productivo.

### 3.10. Seguridad de las Comunicaciones

- (a) **Transferencia de Información.** El Proveedor restringirá el acceso mediante cifrado a los Materiales de Kyndryl almacenados en medios que se transporten físicamente fuera de las Instalaciones. El Proveedor se asegurará de que sea posible verificar y establecer en qué medida los Materiales de Kyndryl han sido o pueden ser transmitidos o puestos a disposición mediante equipos de comunicación de datos.
- (b) **Seguridad de los Servicios de Red.** El Proveedor se asegurará de que se implementen controles y procedimientos de seguridad para todos los servicios y componentes de la red, de acuerdo con las Prácticas Estándar de la Industria, independientemente de si dichos servicios se brindan internamente o se subcontratan.
- (c) **Detección de Intrusiones.** El Proveedor implementará sistemas de detección o prevención de intrusiones y medidas para la prevención y denegación de ataques de servicio para todos los sistemas utilizados para proporcionar los Servicios y Entregables, incluida la vigilancia continua para interceptar y responder a los eventos de seguridad a medida que se identifiquen y actualizar la base de datos de firmas tan pronto como haya nuevas versiones disponibles para distribución comercial.
- (d) **Firewalls.** El Proveedor implementará firewalls que solo permitan el uso de puertos y servicios documentados y aprobados. Todos los demás puertos estarán en modo "denegar todo".
- (e) **Supervisión.** El Proveedor supervisará el uso del acceso privilegiado y mantendrá información de seguridad y medidas de gestión de eventos para: (i) identificar acceso y actividad no autorizados, (ii) facilitar una respuesta oportuna y apropiada a dicho acceso y actividad y (iii) permitir auditorías por parte del Proveedor y Kyndryl.
- (f) **Registro.** El Proveedor deberá emplear procedimientos para garantizar que todos los sistemas, incluidos firewalls, enrutadores, conmutadores de red y sistemas operativos, registren información en sus respectivas instalaciones de registro del sistema o en un sistema de registro centralizado para permitir las auditorías de seguridad a las que se hace referencia a continuación. El proveedor deberá: (i) conservar los registros durante al menos 180 días, (ii) garantizar que ningún registro contenga información confidencial, (iii) proteger los registros contra modificaciones o borrados no autorizados, (iv) realizar copias de seguridad de los registros diariamente y (v) supervisar los registros para detectar riesgos y anomalías funcionales. El Proveedor proporcionará dichos registros a Kyndryl si se lo solicita.

### 3.11. Adquisición, Desarrollo y Mantenimiento de Sistemas

#### (a) Endurecimiento de Aplicaciones

- i) El Proveedor mantendrá e implementará políticas, procedimientos y estándares de desarrollo de aplicaciones seguras consistentes con las Prácticas Estándar de la Industria, como las 25 principales técnicas de desarrollo de seguridad de SANS o el proyecto OWASP Top Ten.
- ii) Todo el Personal del Proveedor responsable del diseño, desarrollo, configuración, prueba e implementación de aplicaciones seguras estará calificado para realizar los Servicios y Entregables y recibirá la capacitación adecuada con respecto a las prácticas de desarrollo de aplicaciones seguras del Proveedor.

#### (b) Endurecimiento del Sistema

- i) El Proveedor establecerá y garantizará el uso de configuraciones seguras estándar de sistemas operativos. Las imágenes deben representar versiones reforzadas del sistema operativo subyacente y las aplicaciones instaladas en el sistema. El endurecimiento incluye la eliminación de cuentas innecesarias (incluidas las cuentas de servicio), la desactivación o eliminación de servicios innecesarios, la aplicación de parches, el cierre de puertos de red abiertos y no utilizados y la implementación de sistemas de detección de intrusiones y/o sistemas de prevención de intrusiones. Estas imágenes deben validarse periódicamente

- para actualizar su configuración de seguridad según corresponda. El Proveedor implementará herramientas y procesos de aplicación de parches tanto para las aplicaciones como para el software del sistema operativo. Cuando ya no sea posible reparar sistemas obsoletos, el Proveedor actualizará a la última versión del software de aplicación. El Proveedor eliminará del sistema el software obsoleto, sin soporte y sin uso.
- ii) El Proveedor limitará los privilegios administrativos únicamente a los miembros del personal que tengan el conocimiento necesario para administrar el sistema operativo y una necesidad comercial para modificar la configuración del sistema operativo subyacente.
  - (c) **Análisis de Vulnerabilidades de Infraestructura.** El Proveedor examinará sus entornos internos (por ejemplo, servidores, dispositivos de red, etc.) relacionados con los Servicios y Entregables mensualmente y los entornos externos relacionados con los Servicios y Entregables semanalmente. El Proveedor tendrá un proceso definido y documentado con plazos específicos para abordar cualquier hallazgo acorde al riesgo planteado y el nivel de gravedad.
  - (d) **Evaluación de Vulnerabilidad de Aplicaciones.** El Proveedor realizará una evaluación de vulnerabilidad de seguridad de cada aplicación antes de cualquier nuevo lanzamiento público. El Proveedor tendrá un proceso definido y documentado para abordar cualquier hallazgo proporcional al riesgo planteado.
  - (e) **Pruebas de Penetración y Evaluaciones de Seguridad.** El Proveedor hará que un tercero independiente reconocido en la industria realice una prueba de penetración integral y una evaluación de seguridad de todos los sistemas involucrados en la prestación de los Servicios y Entregables, de forma periódica y no menos de una vez al año. El Proveedor tendrá un proceso definido y documentado para abordar cualquier hallazgo proporcional al riesgo planteado. Previa solicitud por escrito de Kyndryl, pero no más de una vez al año, el Proveedor proporcionará una certificación que confirme que se ha completado una prueba de penetración de un tercero independiente y que el Proveedor ha implementado un proceso para abordar los hallazgos de acuerdo con una evaluación de riesgos. El Proveedor proporcionará un resumen de los hallazgos, incluido el número de sistemas o aplicaciones puestos a prueba, las fechas de las pruebas, la metodología de las pruebas y el número de hallazgos críticos, altos, medios y bajos.
  - (f) **Recuperación ante Desastres.** Durante la vigencia del Acuerdo, el Proveedor mantendrá una solución de recuperación ante desastres ("DR") o alta disponibilidad ("HA") y un plan relacionado para los Servicios y Entregables que sean consistentes con las Prácticas Estándar de la Industria. El Proveedor probará la solución DR o HA y el plan relacionado al menos una vez al año. Además, la solución y el plan relacionado garantizarán:
    - i) que los sistemas instalados utilizados para proporcionar los Servicios y Entregables se restaurarán en caso de interrupción,
    - ii) la capacidad del Proveedor para restablecer la disponibilidad y el acceso a los Materiales de Kyndryl de manera oportuna en caso de un incidente físico o técnico, y
    - iii) la confidencialidad, integridad, disponibilidad y resiliencia continuas de los sistemas que el Proveedor utiliza para proporcionar los Servicios y Entregables.

### 3.12. Incidentes de Seguridad

- (a) El Proveedor mantendrá y seguirá un programa de respuesta a incidentes de seguridad de la información consistente con las Prácticas Estándar de la Industria, incluidos procedimientos documentados para investigar y abordar incidentes de seguridad de la información. El programa de respuesta a incidentes de seguridad de la información abordará temas como la priorización de incidentes, roles y responsabilidades, procedimientos de escalamiento interno, seguimiento e informes, y contención y corrección. El programa de gestión de incidentes de seguridad de la información se probará, revisará y aprobará en forma periódica, al menos anualmente.
- (b) El Proveedor notificará de inmediato (y en ningún caso tardará más de 48 horas) a Kyndryl después de tener conocimiento de un incidente de seguridad enviando un correo electrónico a [cyber.incidents@kyndryl.com](mailto:cyber.incidents@kyndryl.com). Con respecto a un incidente de seguridad, el Proveedor deberá inmediatamente:
  - i) proporcionar a Kyndryl la información razonablemente solicitada sobre dicho incidente, la investigación del incidente por parte del Proveedor y el estado de cualquier actividad de corrección y restauración del Proveedor. A modo de ejemplo, la información solicitada razonablemente puede conclusiones basadas en hechos relacionadas con la naturaleza, la causa y el impacto del incidente, registros que demuestren acceso privilegiado, administrativo y de otro tipo a Dispositivos, sistemas, servicios o aplicaciones, resúmenes basados en imágenes forenses de Dispositivos, sistemas o aplicaciones, y otros elementos

- similares, en la medida en que sean relevantes para el incidente o las actividades de mitigación, corrección y restauración del Proveedor;
- ii) garantizar que el Personal del Proveedor apropiado con conocimiento del incidente asista a las conferencias telefónicas solicitadas por Kyndryl;
  - iii) contratar a terceros expertos en materia de respuesta a incidentes, gestión de incidentes de filtración de datos, análisis forense y descubrimiento electrónico, previa petición razonable de Kyndryl;
  - iv) proporcionar a Kyndryl asistencia razonable para satisfacer cualquier obligación legal (incluidas las obligaciones de notificar a los reguladores, Interesados, Clientes u otros terceros) de Kyndryl, las filiales de Kyndryl y los Clientes (y sus clientes y filiales); y
  - v) mitigar y corregir de manera oportuna y apropiada los efectos del incidente de seguridad e implementar controles y procesos adicionales para disminuir el riesgo de incidentes similares en el futuro, al tiempo que se presta la debida consideración a cualquier aporte de Kyndryl sobre dichas mitigaciones y correcciones.
- (c) El Proveedor es responsable de todos los costos y gastos incurridos por el Proveedor en la investigación, respuesta, mitigación y corrección de un Incidente de Seguridad. Sujeto a la limitación de responsabilidad del Acuerdo, el Proveedor también es responsable de todos los gastos corrientes incurridos por Kyndryl, las filiales de Kyndryl y los Clientes (y sus clientes y afiliados) en relación con la investigación, respuesta, mitigación y corrección del Incidente de Seguridad. Los costos y gastos de corrección de Incidentes de Seguridad pueden incluir costos relacionados con la detección e investigación del Incidente de Seguridad, determinar responsabilidades conforme a las leyes y normas, volver a cargar datos, corrigiendo defectos del producto (incluso mediante el Código Fuente u otro desarrollo), contratando a terceros para que ayuden con las actividades anteriores u otras actividades pertinentes, y otros costos y gastos que sean necesarios para corregir los efectos nocivos del Incidente de Seguridad.
- (d) En caso de un Incidente de Seguridad que involucre a los Datos Personales de Kyndryl, el Proveedor es responsable de cualquier costo incurrido y reembolsará a Kyndryl todos los costos y gastos en que incurra Kyndryl en relación con:
- i) Proporcionar notificación del Incidente de Seguridad a los reguladores correspondientes, otras agencias de autorregulación gubernamentales y de la industria relevantes, los medios de comunicación (si lo exige la legislación aplicable), los Interesados, los Clientes y otros;
  - ii) Establecer y mantener un centro de llamadas para responder a las preguntas de los Interesados sobre el Incidente de Seguridad y sus consecuencias, durante 1 año después de la fecha en que dichos Interesados fueron notificados del Incidente de Seguridad o durante más tiempo, si así lo exige la legislación de protección de datos aplicable. Kyndryl y el Proveedor trabajarán juntos para crear los guiones y demás materiales que utilizará el personal del centro de llamadas para responder consultas relacionadas con los Datos Personales de Kyndryl; y
  - iii) Proporcionar protección contra el robo de identidad, control de crédito y servicios de restauración de crédito durante 2 años después de la fecha en la que los Interesados afectados por el incidente que elijan registrarse para dichos servicios fueron notificados del Incidente de Seguridad o por más tiempo, si así lo exige la legislación aplicable.
- (e) El Proveedor no identificará, directa ni indirectamente, a Kyndryl ante ningún tercero como afectado por un Incidente de Seguridad, a menos que Kyndryl lo apruebe por escrito o cuando lo requiera la legislación. El Proveedor notificará a Kyndryl por escrito antes de distribuir cualquier notificación requerida legalmente a cualquier tercero, que revelará directa o indirectamente la identidad de Kyndryl.
- (f) El Proveedor también notificará de inmediato a Kyndryl sobre cualquier amenaza real o inminente de infracción de estas Condiciones o sus políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable relacionadas con la entrega de un Entregable o los Servicios.

### 3.13. Relaciones con Proveedores

- (a) **Subcontratistas.** El Proveedor es responsable del cumplimiento de estas Condiciones incluso si utiliza un Subcontratista. El Proveedor comprometerá contractualmente a dichos Subcontratistas a proteger los Materiales de Kyndryl a través de condiciones no menos exhaustivas o estrictas que aquellas que se aplican al Proveedor en las Condiciones. El Proveedor es responsable ante Kyndryl por el desempeño de cada Subcontratista.
- (b) **Gestión de Seguridad y Control de calidad.** El Proveedor realizará el control de calidad y la supervisión de la gestión de seguridad del desarrollo de software subcontratado a un Subcontratista.

- (c) **Información Precontractual.** El Proveedor declara y garantiza que toda la información material proporcionada durante las discusiones precontractuales con Kyndryl relacionadas con la privacidad, seguridad y gestión de datos, ya sea de conformidad con estas Condiciones o de otro modo, es precisa en todos los aspectos materiales y no es, ya sea por omisión o de otro modo, engañosa.

### 3.14. Verificación, Cooperación, Cumplimiento y Evaluación de la Seguridad

- (a) **Verificación** El Proveedor mantendrá un registro auditable que demuestre la conformidad con estas Condiciones.
- (i) Kyndryl, por sí mismo o mediante un auditor externo, puede, previa notificación cursada al Proveedor con 30 días de antelación, verificar que el Proveedor cumpla con estas Condiciones, incluido el acceso a cualquier Instalación o Instalaciones para tales fines, aunque Kyndryl no accederá a ningún centro de datos donde el Proveedor procese los Datos de Kyndryl a menos que tenga una buena razón para creer que con ello proporcionará alguna información relevante. El Proveedor cooperará con la verificación de Kyndryl, incluida la respuesta oportuna y de manera completa a las solicitudes de información, ya sea a través de documentos, otros registros, entrevistas con el Personal del Proveedor relevante o similares. El Proveedor puede ofrecer una prueba de cumplimiento de un código de conducta aprobado o una certificación del sector, o proporcionar información para demostrar el cumplimiento de estas Condiciones, para su consideración por parte de Kyndryl.
  - (ii) No se realizará una verificación más de una vez en un período de 12 meses, a menos que: (A) Kyndryl esté validando la resolución de sospechas del Proveedor derivada de una verificación previa durante el 12.º mes o (B) haya surgido un Incidente de Seguridad y Kyndryl quiera verificar el cumplimiento de las obligaciones relevantes para el Incidente. En cualquier caso, Kyndryl cursará la misma notificación previa por escrito de 30 días como se especifica en el párrafo anterior, pero la urgencia de abordar un Incidente de Seguridad puede requerir que Kyndryl realice una verificación con menos de 30 días de notificación previa por escrito.
  - (iii) Un regulador u otro Controlador, legalmente autorizado, puede ejercer los mismos derechos que Kyndryl en los párrafos (ii) y (iii), bajo el supuesto de que un regulador puede ejercer cualquier derecho adicional que tenga según la legislación vigente.
  - (iv) Si Kyndryl tiene una base razonable para concluir que el Proveedor no cumple con ninguna de estas Condiciones (ya sea que dicha base surja de una verificación bajo estas Condiciones o no), el Proveedor corregirá de inmediato dicho incumplimiento.
  - (v) Esta Sección se aplicará además de la cláusula "Mantenimiento de Registros y Derecho de Auditoría" u otra cláusula de auditoría similar en el Acuerdo.
- (b) **Cooperación.** Si Kyndryl tiene motivos para sospechar que algún Servicio o Entregable puede haber contribuido, está contribuyendo o contribuirá a algún problema de ciberseguridad, el Proveedor cooperará con cualquier consulta de Kyndryl con respecto a dicha sospecha, incluida una respuesta oportuna y de manera completa a las solicitudes de información, ya sea a través de documentos, otros registros, entrevistas al Personal del Proveedor relevante o similares.
- (c) **Cumplimiento de Seguridad.** El Proveedor obtendrá (i) una certificación de cumplimiento respecto de la norma ISO 27001, de una empresa de auditoría pública independiente, (ii) un informe de una empresa de auditoría pública independiente que demuestre su revisión de los sistemas, controles y operaciones del Proveedor de acuerdo con un SOC 2 Tipo 2, que como mínimo incluirá los Principios de Seguridad del Servicio de Confianza (también conocidos como Criterios Comunes), Disponibilidad y Confidencialidad, y (iii) un informe de una empresa de auditoría pública independiente que demuestre su revisión de los sistemas, controles y operaciones del Proveedor de acuerdo con un SOC 1 Tipo 2, si los Servicios afectan a los informes financieros de Kyndryl. El Proveedor cumplirá con las futuras directrices relacionadas con SSAE18 emitidas por la AICPA, la IAASB, la Comisión de Bolsa y Valores o la Contabilidad de Empresas Públicas. A petición, el Proveedor proporcionará rápidamente a Kyndryl una copia de cada certificado e informe que el Proveedor esté obligado a obtener.
- (d) **Evaluación del Cumplimiento de Kyndryl.** Previa solicitud razonable de Kyndryl, pero no más de una vez en cualquier período de 12 meses para cada Servicio o Entregable individual, el Proveedor completará de manera precisa y oportuna (sin exceder los 14 días) un cuestionario para verificar el cumplimiento de sus obligaciones en materia de ciberseguridad y gestión de datos bajo el Acuerdo y estas Condiciones ("**Evaluación del Cumplimiento**"). Si, después de completar la Evaluación del Cumplimiento, Kyndryl determina razonablemente que las prácticas y procedimientos de seguridad y gestión de datos del Proveedor

no cumplen con las obligaciones del Proveedor, Kyndryl notificará al Proveedor las deficiencias. Si el Proveedor está de acuerdo con la evaluación de las deficiencias por parte de Kyndryl, el Proveedor, sin demora injustificada: (i) corregirá dichas deficiencias a su propio costo dentro de un plazo acordado con Kyndryl en función de una evaluación del riesgo y (ii) proporcionará a Kyndryl, o a sus representantes debidamente autorizados, documentación e información razonables que confirmen la corrección de las deficiencias. Si el Proveedor no logra corregir cualquier deficiencia calificada como alta o crítica dentro del plazo acordado, Kyndryl tiene el derecho de rescindir el Documento de Transacción aplicable o el Acuerdo por incumplimiento material inmediatamente después de notificarlo al Proveedor. Kyndryl no revelará la documentación a ningún tercero que no sean sus propios auditores sin el consentimiento por escrito del Proveedor. Si el Proveedor no está de acuerdo con la evaluación de las deficiencias por parte de Kyndryl, el Proveedor proporcionará rápidamente a Kyndryl una explicación por escrito que detalle sus razones y, si Kyndryl no acepta las razones del Proveedor, las partes recurrirán a su respectivo Director de Privacidad, Director de Seguridad de la Información o un ejecutivo con competencia y autoridad similares para una resolución oportuna. Si el uso de los Servicios por parte de Kyndryl causa alguna deficiencia, el Proveedor proporcionará soporte técnico razonable para ayudar a Kyndryl en el uso apropiado de los Servicios para corregir dichas deficiencias.

#### **Article IV. ACCESO A LAS REDES DE KYNDRYL**

Este Artículo se aplica si los empleados del Proveedor tendrán acceso a cualquier Sistema Corporativo.

##### **4.1. Términos generales**

- (a) Kyndryl determinará si autoriza a los empleados del Proveedor a acceder a los Sistemas Corporativos. Si Kyndryl lo autoriza, el Proveedor cumplirá y hará que sus empleados con dicho acceso cumplan, los requisitos de este Artículo.
- (b) Kyndryl identificará los medios por los cuales los empleados del Proveedor pueden acceder a los Sistemas Corporativos, lo que incluye si los empleados tendrán acceso a los Sistemas Corporativos a través de Kyndryl o de los Dispositivos proporcionados por el Proveedor.
- (c) Los empleados del Proveedor solo pueden acceder a los Sistemas Corporativos y solo pueden usar los Dispositivos que Kyndryl autorice para dicho acceso, para proporcionar Servicios, que serán un Dispositivo proporcionado por Kyndryl ("Dispositivo de Kyndryl") o un Dispositivo proporcionado por el Proveedor ("Dispositivo del Proveedor").
- (d) Los empleados del Proveedor no copiarán los Materiales de Kyndryl a los que se pueda acceder a través de un Sistema Corporativo sin la aprobación previa por escrito de Kyndryl (y nunca copiarán los Materiales de Kyndryl a un dispositivo de almacenamiento portátil, como una memoria USB, un disco duro externo u otros elementos similares).
- (e) Previa solicitud, el Proveedor confirmará, mediante el nombre del empleado, los Sistemas Corporativos específicos a los que sus empleados están autorizados a acceder, y han accedido, durante cualquier período de tiempo que Kyndryl identifique.
- (f) El Proveedor notificará a Kyndryl dentro del plazo de veinticuatro (24) horas después de que cualquier empleado del Proveedor con acceso a cualquier Sistema Corporativo: (i) ya no sea empleado del Proveedor o (ii) ya no trabaje en actividades que requieran dicho acceso. El Proveedor trabajará con Kyndryl para garantizar que se revoque de inmediato el acceso de dichos exempleados o empleados actuales.
- (g) El Proveedor notificará inmediatamente a Kyndryl cualquier incidente de seguridad real o presunto (como la pérdida de un Dispositivo de Kyndryl o del Proveedor o el acceso no autorizado a un Dispositivo o datos, materiales u otra información de cualquier tipo) y cooperará con Kyndryl en la investigación de dichos incidentes.
- (h) El Proveedor no puede permitir que un agente, contratista independiente o empleado del subcontratista acceda a ningún Sistema Corporativo sin el consentimiento previo por escrito de Kyndryl; si Kyndryl otorga ese consentimiento, el Proveedor comprometerá contractualmente a estas personas y a sus empleadores para cumplir los requisitos de este Artículo como si estas personas fueran empleados del Proveedor, y será responsable ante Kyndryl de todas las acciones y omisiones de acción de dicha persona o empleador con respecto al acceso al Sistema Corporativo.
- (i) Kyndryl puede revocar el acceso a los Sistemas Corporativos en cualquier momento, para algunos o la totalidad de los empleados del Proveedor, sin previo aviso al Proveedor, a cualquier empleado del Proveedor o a otros, si considera que es necesario para su propia protección.
- (j) Los derechos de Kyndryl no quedan bloqueados, reducidos o restringidos de ninguna manera por ninguna cláusula del Documento de Transacción, el acuerdo base asociado entre las partes ni cualquier otro acuerdo entre las partes, lo que incluye cualquier cláusula que requiera que los datos, materiales u otra información de cualquier tipo residan solo en una ubicación o en ubicaciones seleccionadas o que requiera que solo personas de una ubicación o de ubicaciones seleccionadas accedan a dichos datos, materiales u otra información.

#### **4.2. Software del Dispositivo**

- (a) El Proveedor ordenará a su Personal que instale oportunamente el software en los Dispositivos de Kyndryl y en los Dispositivos del Proveedor que Kyndryl requiera para facilitar el acceso a los Sistemas Corporativos de manera segura. Ni el Proveedor ni su Personal interferirán en las operaciones del software o las características de seguridad que el software permite.
- (b) El Proveedor y su Personal cumplirán con las reglas de configuración de los Dispositivos de Kyndryl y los Dispositivos del Proveedor que Kyndryl establezca y trabajarán con Kyndryl para ayudar a garantizar que el software funcione como Kyndryl lo tenga previsto. Por ejemplo, el Proveedor no anulará el bloqueo de páginas web de software o las características de parches automáticos.
- (c) El Personal del Proveedor no podrá compartir nombres de usuario, contraseñas o similares de los Dispositivos de Kyndryl y los Dispositivos del Proveedor con ninguna otra persona.
- (d) Si Kyndryl autoriza al Personal del Proveedor a acceder a los Sistemas Corporativos utilizando los Dispositivos del Proveedor, el Proveedor instalará y ejecutará un sistema operativo en esos Dispositivos que Kyndryl apruebe y actualizará a una nueva versión de dicho sistema operativo o un nuevo sistema operativo, en un plazo razonable, después de que Kyndryl así lo indique.

### 4.3. Dispositivos de Kyndryl

- (a) Los empleados del Proveedor no pueden utilizar los Dispositivos de Kyndryl para prestar Servicios a ninguna otra persona o entidad, ni para acceder a sistemas de TI, redes, aplicaciones, sitios web, herramientas de correo electrónico, herramientas de colaboración o similares de un Proveedor o un tercero en relación con los Servicios. Los empleados del Proveedor no pueden utilizar los Dispositivos de Kyndryl por ningún motivo personal (por ejemplo, los empleados del Proveedor no pueden almacenar archivos personales como música, videos, imágenes u otros elementos similares en dichos Dispositivos de Kyndryl y no pueden usar Internet desde dichos Dispositivos de Kyndryl por motivos personales). Los empleados del Proveedor no pueden compartir los Dispositivos de Kyndryl con otros empleados del Proveedor que los utilicen para acceder a los Sistemas Corporativos.
- (b) Kyndryl tienen los derechos absolutos para supervisar los Dispositivos de Kyndryl y los Sistemas Corporativos, y corregir posibles intrusiones y otras amenazas de ciberseguridad de cualquier modo, desde cualquier ubicación y utilizando cualquier medio que Kyndryl considere necesario o apropiado, sin previo aviso al Proveedor, a cualquier empleado del Proveedor o a otros. Como ejemplos de tales derechos, Kyndryl puede, en cualquier momento, (i) realizar una prueba de seguridad en cualquier Dispositivo de Kyndryl, (ii) supervisar, recuperar a través de medios técnicos o de otro tipo y revisar comunicaciones (incluidos correos electrónicos de cualquier cuenta de correo electrónico), registros, archivos y otros elementos almacenados en cualquier Dispositivo de Kyndryl o transmitidos a través de cualquier Sistema Corporativo, y (iii) adquirir una imagen forense completa de cualquier Dispositivo de Kyndryl. Si Kyndryl necesita la cooperación del Proveedor para ejercer sus derechos, el Proveedor deberá satisfacer plena y oportunamente las solicitudes de dicha cooperación con Kyndryl (incluidas, por ejemplo, solicitudes para configurar de forma segura cualquier Dispositivo de Kyndryl, instalar software de supervisión o de otro tipo en cualquier Dispositivo de Kyndryl, compartir detalles de conexión a nivel del sistema, participar en medidas de respuesta a incidentes en cualquier Dispositivo de Kyndryl y proporcionar acceso físico a cualquier Dispositivo de Kyndryl para que Kyndryl obtenga una imagen forense completa o de otro tipo, y solicitudes similares y relacionadas).
- (c) Kyndryl retendrá la titularidad de todos los Dispositivos de Kyndryl, y el Proveedor asumirá el riesgo de pérdida de los Dispositivos de Kyndryl, incluidos casos de robo, vandalismo o negligencia. El Proveedor no realizará ni permitirá modificaciones a los Dispositivos de Kyndryl sin el consentimiento previo por escrito de Kyndryl, siendo una modificación cualquier cambio en un Dispositivo, incluido cualquier cambio en el software, las aplicaciones, el diseño de seguridad, la configuración de seguridad o el diseño físico, mecánico o eléctrico del dispositivo.
- (d) El Proveedor devolverá todos los Dispositivos de Kyndryl dentro del plazo de 5 días laborables tras la finalización de la necesidad de dichos Dispositivos para proporcionar los Servicios y, si Kyndryl lo solicita, destruirá todos los datos, materiales y otra información de cualquier tipo en esos Dispositivos al mismo tiempo, sin retener ninguna copia, siguiendo NIST para borrar permanentemente todos esos datos, materiales y otra información. El Proveedor empaquetará y devolverá los Dispositivos de Kyndryl en las mismas condiciones en que fueron entregados al Proveedor, exceptuando el desgaste razonable, responsabilizándose de los costos, en la ubicación que Kyndryl identifique. El incumplimiento por parte del Proveedor de cualquier obligación establecida en este párrafo (d) constituye una infracción sustancial del Documento de Transacción y el acuerdo base asociado y cualquier acuerdo relacionado entre las partes, bajo el supuesto de que un acuerdo está "relacionado" si el acceso a cualquier Sistema Corporativo facilita las tareas del Proveedor u otras actividades bajo ese acuerdo.
- (e) Kyndryl proporcionará soporte para Dispositivos de Kyndryl (incluida la inspección de Dispositivos y el mantenimiento preventivo y correctivo). El Proveedor informará de inmediato a Kyndryl sobre la necesidad de un servicio de reparación.
- (f) Para los programas de software que Kyndryl posea o de los cuales tenga derecho para conceder licencias, Kyndryl otorga al Proveedor un derecho temporal para usar, almacenar y hacer copias suficientes para dar soporte a su uso autorizado de Dispositivos de Kyndryl. El Proveedor no puede transferir programas, hacer copias de la información de la licencia de software, o desensamblar, descompilar, aplicar ingeniería inversa o convertir cualquier programa a menos que la legislación aplicable lo permita sin la posibilidad de renuncia contractual.

## Article V. DEFINICIONES

Es probable que los términos "Servicios" y "Entregables" se definan en el Acuerdo de Relación con el Proveedor o Acuerdo equivalente o un Documento de Transacción; pero si no es así, "**Servicios**" significa cualquier alojamiento, consultoría, instalación, personalización, mantenimiento, soporte, aumento de personal, negocio, trabajo técnico u otro trabajo que el Proveedor realice para Kyndryl, como se especifica en el Documento de Transacción, y "**Entregables**" significa cualquier programa de software, plataforma, aplicación u otros productos o artículos y sus respectivos materiales relacionados que el Proveedor proporcione a Kyndryl, como se especifica en el Documento de Transacción.

- 5.1. **País Adecuado** significa un país que proporciona un nivel adecuado de protección de datos con respecto a la transferencia relevante de conformidad con las leyes de protección de datos aplicables o las decisiones de los reguladores.
- 5.2. **Sistema de IA** significa un sistema basado en máquinas que está diseñado para funcionar con distintos niveles de autonomía y que puede exhibir adaptabilidad después de su implementación, y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar resultados tales como predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales.
- 5.3. **La Información de Contacto Comercial ("BCI", por sus siglas en inglés)** significa los Datos Personales utilizados para contactar, identificar o autenticar a una persona en su calidad profesional o comercial, con fines administrativos y de gestión contractual (p. ej., facturación y administración de cuentas, cálculo de incentivos para socios, informes internos y modelado de negocio, como previsión, ingresos y planificación de capacidad), y para ningún otro fin. Por lo general, la BCI incluye el nombre de una persona, su dirección de correo electrónico comercial, dirección física, número de teléfono u otros datos similares. Por ejemplo, los nombres y direcciones de correo electrónico utilizados para contactar al Personal del Proveedor para servicios de soporte son Información de Contacto Comercial, sin embargo, los nombres y direcciones de correo electrónico incluidos en los datos de soporte de diagnóstico son Datos Personales de Kyndryl.
- 5.4. **Servicio en la nube** significa cualquier oferta "como servicio" que el Proveedor hospede o gestione, incluidas las ofertas de "software como servicio", "plataforma como servicio" e "infraestructura como servicio".
- 5.5. **Controlador** significa la persona física o jurídica, autoridad pública, agencia u otro organismo que, de forma individual o junto con otros, determina los fines y medios del Procesamiento de datos personales.
- 5.6. **Sistema Corporativo** significa al sistema de TI, plataforma, aplicación, red o similar de los que Kyndryl depende para su negocio, incluidos aquellos ubicados o accesibles a través de la intranet de Kyndryl, de Internet o por otros medios.
- 5.7. **Cliente** significa un cliente de Kyndryl.
- 5.8. **Importador de Datos** significa un Procesador o a un Subprocesador que no está establecido en un País Adecuado.
- 5.9. **Interesado** significa una persona física que puede ser identificada, directa o indirectamente.
- 5.10. **Día o Días** refiere a los días calendario, a menos que se designen días "hábiles".
- 5.11. **Dispositivo** significa estación de trabajo, equipo portátil, tablet, teléfono inteligente o asistente digital personal proporcionado por Kyndryl o el Proveedor.
- 5.12. **Instalaciones** significa una ubicación física donde el Proveedor aloja, accede o procesa de otro modo los Entregables o Materiales de Kyndryl.
- 5.13. **Prácticas Estándar de la Industria** significa aquellas prácticas recomendadas o requeridas por el Instituto Nacional de Estándares y Tecnología ("NIST") o la Organización Internacional de Normalización ("ISO"), o cualquier otro organismo u organización con una reputación y sofisticación similares.
- 5.14. **Datos de Kyndryl** significa todos y cada uno de los datos, archivos, materiales, textos, audios, videos, imágenes u otros datos, incluidos los Datos Personales de Kyndryl, la Información de Contacto Comercial de Kyndryl y los Datos no Personales de Kyndryl, que se proporcionan al Proveedor o son accesibles por este (incluido, entre otros, a través de un Servicio en la nube) en relación con la entrega de los Servicios o un Entregable, independientemente de si son proporcionados o puestos a disposición por Kyndryl, el Personal de Kyndryl, un Cliente, un empleado o contratista del Cliente o cualquier otra persona o entidad.
- 5.15. **Materiales de Kyndryl** significa todos y cada uno de los Datos de Kyndryl y la Tecnología de Kyndryl.
- 5.16. **Datos Personales de Kyndryl** significa los Datos Personales, excluyendo la Información de Contacto Comercial de Kyndryl, que Kyndryl proporciona o pone a disposición del Proveedor para la entrega de los Servicios o Entregables. Los Datos Personales de Kyndryl incluyen Datos Personales que Kyndryl controla y Datos Personales que Kyndryl trata en nombre de otros Controladores.
- 5.17. **Tecnología de Kyndryl** significa el Código fuente de Kyndryl, otro código, lenguajes de descripción, firmware, software, herramientas, diseños, esquemas, representaciones gráficas, claves incrustadas, certificados y otra información, materiales, activos, documentos y tecnología que Kyndryl ha otorgado en

- licencia, directa o indirectamente, o que ha puesto a disposición del Proveedor en relación con el Documento de Transacción o el Acuerdo.
- 5.18. **País No Adecuado** significa un país que no se considera adecuado de conformidad con las leyes de protección de datos aplicables o la decisión de un regulador competente.
  - 5.19. **Otro Controlador** significa a cualquier entidad fuera de Kyndryl que sea Responsable del Procesamiento de Datos de Kyndryl, como una filial, un Cliente o la filial de un Cliente de Kyndryl.
  - 5.20. **Software Local** significa el software proporcionado por el Proveedor como un Entregable que Kyndryl o un subcontratista de Kyndryl ejecuta, instala u opera en los servidores o sistemas de Kyndryl o del subcontratista.
  - 5.21. **Datos Personales** significa cualquier información relacionada con un Interesado y cualquier otra información que califique como "datos personales" o similar en virtud de cualquier ley de protección de datos.
  - 5.22. **Personal** significa las personas que son empleados de Kyndryl o del Proveedor, agentes de Kyndryl o del Proveedor, contratistas independientes contratados por Kyndryl o el Proveedor, o proporcionados a una parte por un subcontratista.
  - 5.23. **Procesar o Procesamiento** refiere a cualquier operación o conjunto de operaciones realizadas en los Datos de Kyndryl, incluido el almacenamiento, uso, acceso y lectura.
  - 5.24. **Procesador** significa una persona física o jurídica que procesa datos personales en nombre de un Controlador e incluye "proveedor de servicios" o términos sustancialmente similares bajo cualquier ley de protección de datos.
  - 5.25. **Incidente de Seguridad** significa (a) un suceso que pone en peligro real o inminente la confidencialidad, integridad o disponibilidad de cualquier Material de Kyndryl o un sistema de información utilizado por el Proveedor o sus Subcontratistas para proporcionar los Servicios o Entregables, (b) una infracción de seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal a los Datos de Kyndryl transmitidos, almacenados o Procesados de otra manera, o (c) el acceso no autorizado o uso del Código Fuente que es utilizado por el Proveedor o sus Subcontratistas en la entrega de los Servicios o un Entregable o en relación con esta.
  - 5.26. **Vender** (o **Venta**) significa vender, alquilar, liberar, divulgar, distribuir, poner a disposición, transferir o comunicar de otra forma oral, por escrito o por medios electrónicos u otros, datos por una contraprestación monetaria u otro tipo de contraprestación económica.
  - 5.27. **Compartir** tiene el significado que se le da en la Ley de Privacidad del Consumidor de California de 2018, modificada por la Ley de Derechos de Privacidad del Consumidor de 2020.
  - 5.28. **Cláusulas Contractuales Tipo ("CCT")** significa las cláusulas contractuales requeridas por la legislación de protección de datos aplicable para la transferencia de Datos Personales a los Controladores o Procesadores que no están establecidos en un País Adecuado.
  - 5.29. **Código Fuente** significa código de programación legible por humanos o código que se puede convertir a un formato legible por humanos que los desarrolladores usan para crear, desarrollar o mantener un producto, pero que no se hace público en el curso normal de la distribución o uso comercial del producto.
  - 5.30. **Subprocesador** significa cualquier Subcontratista del Proveedor, incluida una filial del Proveedor, que Procesa los Datos de Kyndryl.
  - 5.31. **Autoridad Supervisora** significa un organismo público independiente responsable de supervisar la aplicación de las leyes de protección de datos dentro de un país o región específicos.