

## TÉRMINOS DE PRIVACIDAD Y SEGURIDAD DEL PROVEEDOR

Estos Términos de Privacidad y Seguridad del Proveedor establecen los derechos y las obligaciones de Kyndryl y del Proveedor en materia de gobierno de datos, seguridad y cuestiones relacionadas (en lo sucesivo, los "**Términos**"). Los Términos se incorporan en el Acuerdo de Relación con el Proveedor, y pasan a formar parte de mismo (o acuerdo equivalente) entre las partes, incluidas las Declaraciones de Trabajo, las Autorizaciones de Trabajo u otros documentos entre nuestras empresas que les hagan referencia (los "**Documentos de Transacción**").

Estos Términos constan de:

- Este documento,
- El Suplemento de Detalles de Tratamiento de datos adjunto a este documento describe las actividades de tratamiento de datos por parte del Proveedor que se derivan de la formalización de estos Términos (para los Documentos de transacción firmados con posterioridad a la formalización de estos Términos, se adjuntará un Anexo de Detalles de Tratamiento de datos separado a cada Documento de transacción, que documentará las actividades de tratamiento de datos por parte del Proveedor específicas de ese documento), y
- Las Cláusulas Contractuales Tipo de la UE, el Anexo sobre las Transferencias Internacionales de Datos del Reino Unido y la Evaluación del Impacto de la Transferencia de Proveedor que se encuentran en <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.

En caso de conflicto entre las disposiciones de estos Términos, el Acuerdo de Relación con el Proveedor, un acuerdo equivalente o un Documento de Transacción, incluido cualquier acuerdo de tratamiento de datos, prevalecerán estos Términos. Si el conflicto es entre estos Términos y las disposiciones acordadas mutuamente entre el Proveedor y Kyndryl para un Cliente de Kyndryl, prevalecerán las disposiciones acordadas mutuamente para un Cliente de Kyndryl.

Las palabras en mayúscula tienen los significados que se indican en el Artículo V de estos Términos, en cualquier otra sección de estos Términos, o en el Documento de Transacción o acuerdo base asociado entre las partes.

### Article I. GOBIERNO DE DATOS E IA

- 1.1. **Cumplimiento de las leyes.** El Proveedor cumplirá con todas las leyes aplicables a los Servicios y Productos, incluidas las leyes relacionadas con la protección de datos, la ciberseguridad y los sistemas de IA. El Proveedor notificará de inmediato a Kyndryl (y en cualquier caso dentro de los plazos requeridos por la ley y brindando 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 de ninguna forma, incluidos los datos agregados, anónimos o de otro tipo, para ningún propósito que no sea el de proporcionar los Servicios y Productos (a modo de ejemplo, el Proveedor no tiene permitido utilizar o reutilizar los Datos de Kyndryl para evaluar la efectividad o los medios para mejorar las ofertas del Proveedor que no sean los Servicios o Productos, para investigación y desarrollo con el fin de crear nuevas ofertas, o para generar informes sobre las ofertas del Proveedor)
  - (b) vender o compartir Datos de Kyndryl; o
  - (c) intentar volver a identificar cualquier información que pueda utilizarse razonablemente para inferir información sobre un Interesado o que de otro modo pueda vincularse al mismo.
- 1.3. **Tecnologías de rastreo web.** Si el Proveedor o sus Subcontratistas, en la entrega de los Servicios o los Productos, recopilan datos utilizando tecnologías de rastreo web (como HTML5, almacenamiento local, etiquetas o tokens de terceros y balizas web), dichos datos se consideran Datos de Kyndryl y el Proveedor deberá cumplir con sus obligaciones con respecto a los Datos de Kyndryl según estos Términos.
- 1.4. **Confidencialidad.** El Proveedor no revelará los Datos de Kyndryl a ningún tercero, salvo a los Subencargados aprobados de conformidad con la Sección 2.5 o a los Subcontratistas aprobados de conformidad con el Acuerdo.
- 1.5. **Acceso del Gobierno.** Si un gobierno, incluido cualquier regulador, exige acceder a los Datos de Kyndryl (por ejemplo, si el gobierno de EE. UU. envía una orden de seguridad nacional al Proveedor para obtener Datos de

Kyndryl), o si la ley requiere de algún otro modo una declaración de Datos de Kyndryl, el Proveedor notificará de inmediato a Kyndryl por escrito sobre dicha demanda o requisito y brindará a Kyndryl una oportunidad razonable para impugnar cualquier declaración, a menos que la ley lo prohíba. Si la notificación está prohibida por ley, el Proveedor tomará las medidas que considere razonablemente apropiadas para impugnar la prohibición y declaración de Datos de Kyndryl mediante acción judicial u otros medios.

- 1.6. **Confidencialidad.** El Proveedor garantiza a Kyndryl que: (a) solo aquellos empleados bajo su cargo que necesiten acceder a los Datos de Kyndryl para proporcionar Servicios o Productos tendrán dicho acceso, y solo en la medida necesaria; y (b) ha obligado a sus empleados a suscribir acuerdos de confidencialidad que exigen que esos empleados utilicen y revelen los Datos de Kyndryl únicamente en la medida en que lo permitan estos Términos.
- 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 propio cargo, cuando se rescinda o venza el Documento de Transacción, o antes a petición de Kyndryl. Si Kyndryl solicita suprimir los datos, el Proveedor, de conformidad con NIST SP 800-88 rev.1, hará que los datos queden ilegibles y no puedan recomponerse ni reconstruirse, y certificará la eliminación a Kyndryl bajo petición. Si Kyndryl requiere la devolución de Datos de Kyndryl, el Proveedor lo hará en un formato comúnmente utilizado según el plazo razonable y las instrucciones de Kyndryl.
- 1.8. **Sistemas de IA**
  - (a) El Proveedor no deberá utilizar Sistemas de IA en la entrega de los Servicios o un Producto ni incluir Sistemas de IA en un Producto, sin autorización previa de Kyndryl en un Documento de Transacción o en el Acuerdo. Al solicitar autorización de Kyndryl, el Proveedor le proporcionará a Kyndryl por escrito toda información necesaria para evaluar el uso por parte del Proveedor de Sistemas de IA (por ejemplo, los flujos de datos, los modelos de lenguaje utilizados, la separación de datos).
  - (b) El Proveedor declara y garantiza que: (i) tanto la entrada proporcionada por Kyndryl (incluyendo la entrada proporcionada por los empleados o cualquier otro tercero sujeto a un Documento de Transacción) como la salida se clasificarán 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 durante un plazo superior al necesario para proporcionar los Servicios, (iv) los Sistemas de IA (incluyendo los resultados y los datos de entrenamiento) se clasificarán como parte de los Servicios, y (v) en la medida permitida por la legislación aplicable, el Proveedor por la presente asigna todos sus derechos, título e interés sobre los resultados de los Sistemas de IA a Kyndryl.
  - (c) El Proveedor deberá implementar y mantener un programa documentado de gobierno y gestión de riesgos para los Sistemas de IA que identifique, pruebe, supervise y mitigue razonable y apropiadamente los riesgos conocidos y previsible, incluidos, entre otros, los riesgos relacionados con la ética, el sesgo, la seguridad y la protección asociados con, o derivados de, los Sistemas de IA. Previa solicitud, el Proveedor compartirá una copia de su programa de gobierno y gestión de riesgos para Sistemas de IA. El Proveedor notificará de inmediato a Kyndryl por escrito sobre cualquier riesgo en que se haya incurrido o cualquier riesgo material que se haya identificado de conformidad con la disposición sobre notificaciones acordada en el Documento de Transacción con una copia a [ailegalteam@kyndryl.com](mailto:ailegalteam@kyndryl.com).

## Article II. PRIVACIDAD

- 2.1. **Información de Contacto Comercial (BCI).** Kyndryl y el Proveedor pueden Tratar la BCI de la otra parte de conformidad con las leyes de protección de datos aplicables como Responsables independientes dondequiera que hagan negocios para suministrar y recibir los Productos y los Servicios. Las partes no actúan como Responsables conjuntos en relación con la BCI de la otra parte. Si cualquiera de las partes informa a la otra parte acerca de la solicitud de un Interesado con respecto a la BCI de la otra parte, esta será responsable de dar respuesta a dicha solicitud directamente al Interesado. Cada una de las partes ha implementado medidas técnicas y organizativas apropiadas para proteger la BCI de la otra parte. Para mayor claridad, la Sección 3.12 (Incidencias de seguridad) se aplica a la BCI.
- 2.2. **Proveedor como Encargado.** Kyndryl designa al Proveedor como Encargado del Tratamiento de Datos Personales de Kyndryl con el único propósito de proporcionar los Productos y Servicios de acuerdo con las instrucciones de Kyndryl, incluidas aquellas contenidas en estos Términos, el Acuerdo y cualquier Documento

de Transacción relacionado. El Proveedor es un Encargado del Tratamiento de Datos Personales de Kyndryl. Si el Proveedor no actúa de acuerdo con las instrucciones de Kyndryl para que Kyndryl pueda cumplir con ley de protección de datos aplicable, Kyndryl podrá rescindir la parte afectada de los Servicios mediante una notificación por escrito. Si el Proveedor cree que alguna instrucción incumple una ley de protección de datos, el Proveedor informará a Kyndryl de inmediato y según el plazo requerido por ley.

**2.3. Medidas técnicas y organizativas.** El Proveedor implementará y mantendrá las medidas técnicas y organizativas oportunas, incluidas las medidas de seguridad especificadas en el Artículo III a continuación, con el objetivo de garantizar un nivel de seguridad apropiado al riesgo asociado con la entrega de los Servicios y Productos.

**2.4. Derechos y solicitudes de los Interesados**

- (a) El Proveedor informará a Kyndryl sin demora (en un plazo que permita a Kyndryl y a cualquier Otro Responsable cumplir con sus obligaciones legales) acerca de cualquier solicitud de un Interesado que desee ejercer cualquier derecho del Interesado (por ejemplo, la rectificación, supresión o bloqueo de los datos) con respecto a los Datos Personales de Kyndryl. El Proveedor también puede remitir de inmediato a un Interesado a que realice dicha solicitud a Kyndryl. El Proveedor no responderá a ninguna solicitud de los Interesados a menos que Kyndryl lo requiera legalmente o le indique por escrito que lo haga.
- (b) Si Kyndryl está obligado a proporcionar información sobre los Datos Personales de Kyndryl a Otros Responsables u otros terceros (por ejemplo, Interesados o reguladores), el Proveedor asistirá a Kyndryl proporcionando información y tomando otras medidas razonables que Kyndryl solicite, en un plazo que permita a Kyndryl responder oportunamente a dichos Otros responsables o terceros.

**2.5. Subencargados**

- (a) Kyndryl autoriza al Proveedor a contratar a los Subencargados que se relacionan en los respectivos Suplementos de Detalles de Tratamiento de Datos. El Proveedor también podrá contratar Subencargados adicionales o sustitutos, o ampliar el alcance del Tratamiento de Datos por parte de un Subencargado existente, en virtud de las condiciones siguientes:
  - (i) El Proveedor proporcionará a Kyndryl un aviso previo por escrito antes de proceder con cualquier cambio.
  - (ii) Kyndryl puede oponerse a la contratación de cualquier Subencargado nuevo o sustituto, así como a la ampliación del alcance por motivos razonables, y las partes colaborarán de buena fe para atender la objeción de Kyndryl.
  - (iii) Sin perjuicio del derecho de Kyndryl a oponerse en cualquier momento, el Proveedor puede proceder con el cambio si Kyndryl no ha presentado ninguna objeción en un plazo de 30 días a partir de la fecha del aviso por escrito del Proveedor.
- (b) El Proveedor impondrá las obligaciones de protección de datos, seguridad y certificación que se establecen en estos Términos a cada Subencargado aprobado antes de que dicho Subencargado realice cualquier Tratamiento de Datos Personales de Kyndryl. El Proveedor es completamente responsable ante Kyndryl por el cumplimiento de las obligaciones de cada Subencargado.

**2.6. Tratamiento transfronterizo de datos**

- (a) El Proveedor no transferirá ni revelará (tampoco mediante acceso remoto) Datos Personales de Kyndryl entre fronteras, excepto a los Subencargados aprobados de acuerdo con la Sección 2.5. Si Kyndryl aprueba la transferencia transfronteriza de Datos Personales de Kyndryl, las partes cooperarán para cumplir con las leyes de protección de datos aplicables. Si dichas leyes exigen las CCT, el Proveedor suscribirá las CCT de inmediato, según se define a continuación.
- (b) **Espacio Económico Europeo**
  - (i) Si Kyndryl transfiere Datos Personales sujetos al Reglamento General de Protección de Datos (2016/679) fuera del Espacio Económico Europeo a un Proveedor no establecido 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 que se encuentran en <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms> ("CCT de la UE").
  - (ii) En caso de que Kyndryl haya desaparecido de facto, haya dejado de existir jurídicamente o sea insolvente, los Otros Responsables tendrán derecho a rescindir el Acuerdo y a dar instrucciones al Proveedor para el borrado o la devolución de los Datos Personales de Kyndryl.

- (iii) La evaluación de Kyndryl sobre las transferencias de Datos Personales a Proveedores según lo exigen las CCT de la UE están publicadas para la revisión del Proveedor en <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.
  - (iv) El Proveedor proporcionará detalles suficientes de cada Subencargado en los Suplementos de Detalles de Tratamiento de Datos y avisos para satisfacer sus obligaciones como importador de datos según la cláusula 14(c) de las Cláusulas Contractuales Tipo de la UE, incluido el nombre del Subencargado y el lugar del tratamiento de datos y las actividades de tratamiento de datos.
  - (v) El Proveedor actuará como Exportador de Datos y suscribirá las Cláusulas Contractuales Tipo de la UE u otro mecanismo de transferencia apropiado con cada Subencargado aprobado que no esté establecido en un País Adecuado.
- (c) **Reino Unido.** Si se transfieren Datos Personales de Kyndryl sujetos a la Ley de Protección de Datos del Reino Unido (2018) fuera del Reino Unido a un País No Adecuado, el Proveedor por la presente acepta el Anexo sobre Transferencias Internacionales de Datos del Reino Unido, firmado previamente por Kyndryl y que se encuentra en <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.
- (d) **Suiza.** Si se transfieren Datos Personales de Kyndryl sujetos a la Ley Federal Suiza sobre Protección de Datos ("FADP") fuera de Suiza a un País No Adecuado, el Proveedor por la presente suscribe las Cláusulas Contractuales Tipo de la UE, en virtud de las modificaciones siguientes:
- (i) las referencias al RGPD también incluirán la referencia a las disposiciones equivalentes de la FADP;
  - (ii) la Comisión Federal Suiza de Información y Protección de Datos es la autoridad de control exclusiva de conformidad con la cláusula 13 y el Anexo I.C de las CCT de la UE;
  - (iii) La ley aplicable de conformidad 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 forma que excluya a los interesados en Suiza de la posibilidad de demanda por vulneración de 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 a un Proveedor que no esté establecido en un País Adecuado, el Proveedor por la presente acepta el Anexo II de la Resolução CD/ANPD nº 19/2024 (en adelante, "Cláusulas Contractuales Tipo de Brasil" o "CCT de Brasil"), previamente firmado por Kyndryl y que se encuentra en <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms> ("CCT 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 la Autoridad de Control no ha publicado las Cláusulas Contractuales Tipo locales (por ejemplo, la Ley de Protección de Datos de Perú, la Ley de Protección de Datos de Sudáfrica) o dicha Autoridad de Control ha aprobado el uso de las cláusulas contractuales tipo de la UE como una medida de protección suficiente para las transferencias transfronterizas (por ejemplo, la Ley de Protección de Datos de Argentina), las Cláusulas Contractuales Tipo de la UE registrarán dicha transferencia sin perjuicio de las modificaciones siguientes:
- (i) Las referencias al RGPD también incluirán la referencia a las disposiciones equivalentes de la ley de protección de datos local;
  - (ii) la Autoridad de Control local es la autoridad de control exclusiva de conformidad con la Cláusula 13 y el Anexo I.C de las CCT de la UE;
  - (iii) La ley aplicable de conformidad con la cláusula 17 de las CCT de la UE será la ley de protección de datos local; y
  - (iv) El término "estado miembro" no debe interpretarse de forma que excluya a los interesados de la posibilidad de demanda por vulneración de 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 Tratamiento, el Proveedor asistirá a Kyndryl con las Medidas Técnicas y Organizativas ("TOM") apropiadas para el cumplimiento de las obligaciones asociadas con las solicitudes y los derechos del Interesado. El Proveedor también asistirá a Kyndryl para garantizar el cumplimiento de las obligaciones relativas a la seguridad del Tratamiento, la notificación y la comunicación de cualquier incidencia de seguridad y la creación de evaluaciones del impacto de la protección de datos, incluida la consulta previa con el regulador responsable, si se requiere, teniendo en cuenta la información disponible para el Proveedor.

- (b) El Proveedor mantendrá un registro actualizado del nombre y los datos de contacto de cada Subencargado, incluido el representante de cada Subencargado y el delegado de protección de datos. Previa solicitud, el Proveedor proporcionará este registro a Kyndryl en un plazo que permita a Kyndryl responder oportunamente a cualquier demanda de un Cliente u otros terceros.

## 2.8. Términos requeridos por país

### (a) **Japón**

- i) Para la BCI de Interesados ubicados en Japón, el Proveedor cumplirá con las disposiciones de estos Términos, aplicables al Proveedor como Encargado.
- ii) La definición de "Incidencia de seguridad" en estos Términos se modifica en el presente documento para incluir las infracciones de los Datos Personales de Kyndryl de las que se tenga sospecha razonable y que estén relacionadas con Interesados ubicados en Japón.
- iii) El Proveedor garantiza que no tiene ningún motivo para creer que las leyes y prácticas de algún país donde el Proveedor o sus Subencargados traten Datos Personales de Kyndryl impidan al Proveedor cumplir con sus obligaciones en virtud de estos Términos. El Proveedor notificará a Kyndryl si, después de haber aceptado los Términos y durante la vigencia de estos, el Proveedor tiene algún motivo para creer que no puede cumplir con su obligación en virtud de los Términos. En este caso, las partes cooperarán de buena fe para identificar las medidas apropiadas a adoptar para resolver la situación. Si no se pueden implementar las medidas apropiadas, Kyndryl evaluará si debe suspender la transferencia de Datos Personales de Kyndryl.

- (b) **California.** Cuando el Proveedor, como Encargado, realice el Tratamiento de Datos Personales de Kyndryl de Interesados ubicados en el Estado de California, (i) Kyndryl revelará los Datos Personales de Kyndryl al Proveedor solo para los fines comerciales limitados y especificados seleccionados en el Suplemento de Detalles de Tratamiento de Datos aplicable, (ii) Kyndryl puede, previo aviso, tomar medidas razonables y apropiadas para detener el Tratamiento no autorizado o para garantizar que el Tratamiento por parte del Proveedor sea consecuente con las obligaciones de Kyndryl en virtud de las leyes de protección de datos aplicables, y (iii) el Proveedor no retendrá, utilizará o revelará Datos Personales de Kyndryl fuera de la relación comercial directa entre Kyndryl y el Proveedor.

### (c) **Canadá.**

- i) Para la BCI de los Interesados ubicados en Canadá, el Proveedor cumplirá con las disposiciones de estos Términos, aplicables al Proveedor como Encargado, en la medida en que se consideren Datos Personales.
- ii) Para mayor claridad, las referencias a las leyes de protección de datos aplicables incluyen, entre otras, todas las pautas y buenas prácticas legalmente vinculantes publicadas por una Autoridad de Control en Canadá que tenga jurisdicción, según sean enmendadas, reemplazadas o sustituidas.
- iii) El Proveedor no utilizará los Datos de Kyndryl para crear una base de datos de características biométricas y/o mediciones con fines de identificación personal.
- iv) El Proveedor llevará a cabo cualquier evaluación del impacto sobre la privacidad o evaluación del impacto de la transferencia requerida según las leyes de protección de datos de Canadá, proporcionará una copia de dichas evaluaciones cuando se solicite y notificará a Kyndryl sin dilación 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 las medidas complementarias, 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 rescindir los servicios del Proveedor en cuestión sin indemnización.
- vi) El Proveedor prestará asistencia a Kyndryl proporcionando la información adicional que sea razonablemente solicitada para que Kyndryl lleve a cabo su propia evaluación, conforme a las leyes de protección de datos aplicables en Canadá, sobre si los Términos brindan 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 dirección del Proveedor y serán coherentes con las Prácticas Estándares del Sector, como el Instituto Nacional de Estándares y Tecnología (NIST) o la International Organization for Standardization (ISO). El Proveedor revisará y evaluará las políticas de seguridad de la información del Proveedor al menos una vez al año, inmediatamente después de que se realicen cambios significativos en las políticas, con el fin de confirmar la continuidad de su aplicabilidad y eficacia. El Proveedor no realizará cambios en las políticas que puedan degradar la seguridad del Proveedor con respecto a los Materiales de Kyndryl, los Productos o los Servicios.
- (b) **Pruebas.** El Proveedor mantendrá un proceso para probar periódicamente la eficacia de sus medidas técnicas y organizativas con el fin de garantizar la seguridad de los Materiales de Kyndryl, los Productos y los Servicios.
- (c) **Gestión de riesgos.** El Proveedor realizará las correspondientes evaluaciones del riesgo de seguridad de la información como parte de un programa continuo de gobierno del riesgo con los siguientes objetivos: (i) identificar el riesgo de seguridad de la información relacionado con los Materiales de Kyndryl, los Productos y los Servicios; (ii) evaluar el impacto de dicho riesgo; y (iii) cuando se identifiquen o justifiquen estrategias de reducción o mitigación de riesgos, implementar medidas para mitigar y gestionar eficazmente dicho riesgo reconociendo que el panorama de amenazas cambia constantemente.

### 3.2. Seguridad del personal

- (a) **Capacitación en seguridad.** El Proveedor proporcionará cursos de sensibilización, formación y capacitación en seguridad y privacidad adecuados al menos una vez al año a todo el Personal del Proveedor que tenga acceso, o posibilidad de acceso, a los Materiales de Kyndryl, los Productos o los Servicios.
- (b) **Verificación de antecedentes.** El Proveedor mantendrá y seguirá los requisitos estándares de verificación laboral obligatorios para todos los nuevos empleados contratados y extenderá dichos requisitos a todo el Personal del Proveedor y de las subsidiarias controladas por el Proveedor. Estos requisitos incluirán comprobaciones de antecedentes penales en la medida permitida por las leyes locales, pruebas de validación de identidad y las verificaciones adicionales que el Proveedor considere oportunas. El Proveedor repetirá y revalidará periódicamente estos requisitos, según considere necesario.

### 3.3. Gestión de activos

- (a) **Inventario de activos.** El Proveedor mantendrá un inventario de activos de todos los equipos donde se almacenen Materiales de Kyndryl. El Proveedor restringirá el acceso a dichos equipos únicamente al Personal autorizado del Proveedor. El Proveedor impedirá el acceso sin autorización y la copia, modificación o eliminación de los Materiales de Kyndryl. El Proveedor mantendrá medidas para impedir el acceso sin autorización, la copia, la modificación o la supresión de los Materiales de Kyndryl.
- (b) **Seguridad de los componentes de software.** El Proveedor se compromete a realizar adecuadamente un inventario de todos los componentes de software (incluido el software de código abierto) utilizados en la prestación de los Servicios y el desarrollo y el suministro de los Productos. El Proveedor evaluará si dichos componentes de software contienen defectos de seguridad y/o vulnerabilidades que podrían causar la divulgación o el acceso no autorizados a los Materiales de Kyndryl, los Productos o los Servicios. El Proveedor realizará dicha evaluación antes de entregar o proporcionar a Kyndryl acceso a los Servicios y Productos y de forma continua posteriormente durante el plazo indicado en el Documento de Transacción. El Proveedor se compromete a remediar oportunamente cualquier defecto o vulnerabilidad de seguridad en cualquier componente de software del que tenga conocimiento. El Proveedor responderá sin demora a cualquier consulta de Kyndryl respecto a si el Proveedor conoce algún defecto o vulnerabilidad de seguridad en dicho componente de software y/o ha sido corregido por el Proveedor.

**3.4. Política de control de accesos.** El Proveedor mantendrá una política de control de accesos basada en roles apropiada y medidas técnicas de control de accesos apropiadas acordes con las Prácticas Estándares del Sector para restringir el acceso a los Materiales de Kyndryl y a los activos del Proveedor utilizados para proporcionar los Servicios únicamente al Personal autorizado del Proveedor y limitar dicho acceso al nivel mínimo requerido para proporcionar y respaldar los Servicios y los Productos. Dicho acceso se registrará de acuerdo con los requisitos enumerados en 3.10(f).

### 3.5. Autorización

- (a) El Proveedor mantendrá procedimientos de creación y supresión de cuentas de usuario para otorgar y revocar rápidamente (y en cualquier caso en un plazo de veinticuatro (24) horas) el acceso a todos los Materiales de Kyndryl y a todas las aplicaciones y todos los activos internos del Proveedor utilizados en la prestación de los Servicios y Productos. El Proveedor asignará una autorización apropiada para aprobar la creación y revocación de cuentas de usuario o niveles elevados o reducidos de acceso para las cuentas existentes, incluyendo la rescisión del empleo del Personal, contrato, compromiso u otro acuerdo con el Proveedor o un cambio de función si dicho Personal ya no requiere dichos derechos de acceso.
- (b) El Proveedor mantendrá y actualizará los registros del Personal del Proveedor que esté autorizado a acceder a los sistemas y activos en los cuales se almacenen los Materiales de Kyndryl y los Productos, o desde los cuales se pueda acceder a ellos, o que se utilicen para proporcionar los Servicios, y revisará dichos registros al menos trimestralmente. Se permitirá al Personal administrativo y de soporte técnico acceder a dichos sistemas, a los Materiales de Kyndryl y a los Productos únicamente cuando sea necesario y siempre que dicho Personal cumpla con las medidas técnicas y organizativas del Proveedor aplicables.
- (c) El Proveedor garantizará que las cuentas de usuario que tengan acceso a dichos sistemas y activos sean exclusivas 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 activos y sistemas de información.
- (b) El Proveedor mantendrá prácticas de protección por contraseña acordes con las Prácticas Estándares del Sector y diseñadas para mantener la confidencialidad y la integridad de las contraseñas generadas, asignadas, distribuidas y almacenadas en cualquier formato. El Proveedor generará o requerirá que el usuario cree y utilice una contraseña o frase de contraseña compleja fuerte generada aleatoriamente o alternativas adecuadas, como certificados digitales, tarjetas/tokens de hardware o biométrica.
- (c) El Proveedor utilizará la autenticación multifactor, incluso para el acceso administrativo al portal en la nube y al dominio. La autenticación multifactor puede incluir técnicas como el uso de certificados criptográficos, tokens de contraseña de un solo uso (OTP) o biométrica.

### 3.7. Criptografía

- (a) **Política.** El Proveedor implementará y mantendrá políticas y estándares criptográficos acordes con las Prácticas Estándares del Sector para proteger los Materiales de Kyndryl, incluyendo, cuando corresponda, la seudonimización y el cifrado.
- (b) **Cifrado.** El Proveedor cifrará los materiales Kyndryl en tránsito y en reposo. Los algoritmos de cifrado protegerán los datos a niveles de seguridad acordes con las Prácticas Estándares del Sector (como NIST SP 800-131a) y utilizarán funciones hashing reconocidas del sector, que tengan como mínimo la misma protección que el cifrado Advanced Encryption Standard 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 acordes con las Prácticas Estándares del Sector que definan los principales requisitos de cifrado, seguridad, rotación y de ciclo vital, incluida la creación, la distribución, la revocación, el archivado y la destrucción.

### 3.8. Seguridad física y medioambiental

- (a) **Acceso a las instalaciones.** El Proveedor limitará el acceso a las Instalaciones a su Personal autorizado.
- (b) **Protección contra interrupciones.** El Proveedor realizará los esfuerzos que sean razonables para proteger dichos sistemas y activos contra cortes de electricidad y otras interrupciones causadas por anomalías en los suministros públicos.
- (c) **Eliminación o reutilización segura de equipos.** El proveedor se asegurará de que todos los Materiales de Kyndryl se hayan sobrescrito o eliminado de forma segura del equipo que contiene el soporte de almacenamiento utilizando procesos acordes con las Prácticas Estándares del Sector antes de la eliminación o reutilización de dicho equipo.

### 3.9. Seguridad de las 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 el malware.** El Proveedor implementará soluciones antivirus y de gestión de puntos finales para mantener controles antimalware con el fin de proteger dichos sistemas y activos contra el software malicioso, incluido el software malicioso que se origina en las redes públicas.

- (c) **Gestión de la configuración.** El Proveedor tendrá políticas que regirán la instalación de software y utilidades por parte del Personal.
- (d) **Gestión de cambios.** El Proveedor mantendrá e implementará procedimientos para garantizar que únicamente se implementen en los entornos de producción las versiones aprobadas y seguras del código, las configuraciones, los sistemas y las aplicaciones.
- (e) **Separación lógica.** El Proveedor mantendrá el aislamiento apropiado de su entorno de producción, de no producción u otros y, si los Materiales de Kyndryl ya están presentes o se han transferido a un entorno de no producción (p. ej., para reproducir un error), el Proveedor se asegurará de que las protecciones de seguridad y privacidad en el entorno de no producción sean iguales a las del entorno de producción.

### 3.10. Seguridad de las comunicaciones

- (a) **Transferencia de información.** El Proveedor restringirá el acceso mediante cifrado a los Materiales de Kyndryl almacenados en soportes que se transporten físicamente fuera de las Instalaciones. El Proveedor se asegurará de que sea posible verificar y establecer hasta qué punto los Materiales de Kyndryl se transmiten o han transmitido o están o han estado disponibles, a través de equipos de comunicación de datos.
- (b) **Seguridad de los servicios de red.** El Proveedor se asegurará de que se hayan implementado controles y procedimientos de seguridad para todos servicios y componentes de red acordes con las Prácticas Estándares del Sector, independientemente de si la prestación de dichos servicios se realiza internamente o se subcontrata.
- (c) **Detección de intrusiones.** El Proveedor implementará sistemas de detección de intrusiones o prevención de intrusiones y medidas de prevención contra los ataques de denegación de servicio para todos los sistemas utilizados con el fin de proporcionar los Servicios y Productos, incluida la vigilancia continua para interceptar y responder a sucesos de seguridad a medida que se identifican, y actualizar la base de datos de firmas tan pronto como estén disponibles nuevas versiones para la distribución comercial.
- (d) **Cortafuegos.** El Proveedor implementará cortafuegos que únicamente permitan la utilización de los puertos y servicios documentados y aprobados. Todos los demás puertos estarán en modo "denegar todo".
- (e) **Supervisión.** El Proveedor supervisará la utilización del acceso privilegiado y mantendrá información de seguridad y medidas de gestión de eventos para: (i) identificar el acceso y la actividad no autorizada, (ii) facilitar una respuesta oportuna y adecuada a dicho acceso y actividad, y (iii) permitir auditorías por parte del Proveedor y Kyndryl.
- (f) **Registro.** El Proveedor empleará los procedimientos necesarios para garantizar que todos los sistemas, incluidos cortafuegos, enrutadores, conmutadores de red y sistemas operativos, registran información en su correspondiente recurso de registro del sistema o en un sistema de registro centralizado con el fin de 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 diariamente la copia de seguridad de los registros, y (v) supervisar los registros para detectar los riesgos y anomalías funcionales. El Proveedor proporcionará dichos registros a Kyndryl si así se lo solicita.

### 3.11. Adquisición, desarrollo y mantenimiento de sistemas

#### (a) Refuerzo de las aplicaciones

- i) El Proveedor mantendrá e implementará políticas, procedimientos y estándares de desarrollo de aplicaciones seguras acordes con las Prácticas Estándares del Sector, como las 25 principales técnicas de desarrollo de seguridad de SANS o el proyecto Top Ten de OWASP.
- ii) Todo el Personal del Proveedor responsable del diseño, el desarrollo, la configuración, las pruebas y la implementación de aplicaciones seguras estará cualificado para suministrar los Servicios y Productos y recibirá la formación adecuada con respecto a las prácticas de desarrollo de aplicaciones seguras del Proveedor.

#### (b) Refuerzo del sistema

- i) El Proveedor establecerá y garantizará el uso de configuraciones seguras estándares de los sistemas operativos. Las imágenes deben representar versiones reforzadas del sistema operativo subyacente y las aplicaciones instaladas en el sistema. El refuerzo incluye la eliminación de cuentas innecesarias (incluidas las cuentas de servicio), la desactivación o eliminación de los servicios innecesarios, la aplicación de parches, el cierre de los puertos de red abiertos y no utilizados y la implementación de sistemas de detección o 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 se pueden aplicar parches a los sistemas obsoletos, el Proveedor actualizará a la última versión del software de la aplicación. El Proveedor eliminará del sistema el software obsoleto, incompatible y no utilizado.
- ii) El Proveedor limitará los privilegios administrativos únicamente al personal que tenga los conocimientos necesarios para administrar el sistema operativo y también una necesidad comercial de modificar la configuración del sistema operativo subyacente.
- (c) **Análisis de vulnerabilidades de la infraestructura.** El Proveedor realizará una exploración mensual de sus entornos internos (p. ej., servidores, dispositivos de red, etc.) relacionados con los Servicios y Productos y una exploración semanal de los entornos externos relacionados con los Servicios y Productos. El Proveedor tendrá un proceso definido y documentado con plazos específicos para abordar los hallazgos acorde al riesgo planteado y al nivel de gravedad.
  - (d) **Evaluación de vulnerabilidades de las aplicaciones.** El Proveedor realizará una evaluación de vulnerabilidades de seguridad de las aplicaciones antes de cualquier nueva exposición pública. El Proveedor tendrá un proceso definido y documentado para abordar los hallazgos acorde al riesgo planteado.
  - (e) **Pruebas de penetración y evaluaciones de seguridad.** El Proveedor contará con un tercero independiente reconocido por el sector para realizar una prueba de penetración integral y una evaluación de seguridad de todos los sistemas involucrados en la prestación de los Servicios y Entregables de manera recurrente, al menos una vez al año. El Proveedor tendrá un proceso definido y documentado para abordar los hallazgos acorde al riesgo planteado. Tras la solicitud por escrito de Kyndryl, pero no más de una vez por año, el Proveedor proporcionará una testificación que confirme que se ha completado una prueba de penetración independiente por parte de terceros 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 probados, las fechas de las pruebas, la metodología de las pruebas y el número de hallazgos de gravedad crítica, alta, media y baja.
  - (f) **Recuperación tras desastre.** Durante la vigencia del Acuerdo, el Proveedor mantendrá una solución de recuperación tras desastre ("DR") o alta disponibilidad ("HA") y un plan relacionado para los Servicios y Productos acordes con las Prácticas Estándares del Sector. El Proveedor probará la solución DR o HA y el plan relacionado al menos una vez al año. Asimismo, la solución y el plan relacionado garantizarán:
    - i) que los sistemas instalados utilizados para proporcionar los Servicios y Productos 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 una incidencia física o técnica, y
    - iii) la confidencialidad, integridad, disponibilidad y resiliencia constantes de los sistemas que el Proveedor utiliza para proporcionar los Servicios y Productos.

### 3.12. Incidencias de seguridad

- (a) El Proveedor mantendrá y seguirá un programa de respuesta a incidencias de seguridad de la información acordes con las Prácticas Estándares del Sector, incluidos los procedimientos documentados para investigar y abordar las incidencias de seguridad de la información. El programa de respuesta a incidencias de seguridad de la información abordará temas tales como la priorización de las incidencias, los roles y responsabilidades, los procedimientos de escalamiento interno, el rastreo y la elaboración de informes, así como la contención y la corrección. El programa de gestión de incidencias de seguridad de la información deberá probarse, revisarse y aprobarse periódicamente, pero al menos una vez al año.
- (b) El Proveedor notificará a Kyndryl de inmediato (y en ningún caso en un plazo superior a 48 horas) después de tener conocimiento de una incidencia de seguridad mediante el envío de un correo electrónico a [cyber.incidents@kyndryl.com](mailto:cyber.incidents@kyndryl.com). Con respecto a una incidencia de seguridad, el Proveedor deberá, de inmediato:
  - i) proporcionar a Kyndryl la información razonablemente solicitada sobre dicha incidencia, la investigación de la incidencia por parte del Proveedor y el estado de cualquier actividad de corrección y restauración por parte del Proveedor. A modo de ejemplo, la información solicitada razonablemente puede incluir los hallazgos fácticos relacionados con la naturaleza, la causa y el impacto de la incidencia, registros que demuestren el 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 la incidencia o las actividades de mitigación, corrección y restauración del Proveedor;

- ii) garantizar que Personal apropiado del Proveedor con conocimiento de la incidencia asista a las conferencias telefónicas solicitadas por Kyndryl;
  - iii) involucrar a expertos externos de respuesta a incidencias, gestión de incidencias de violación de la seguridad de los datos, análisis forense y descubrimiento electrónico, a petición razonable de Kyndryl;
  - iv) proporcionar a Kyndryl asistencia razonable para satisfacer las obligaciones legales (incluidas las obligaciones de notificación a los reguladores, los Interesados, el Cliente u otros terceros) de Kyndryl, los afiliados de Kyndryl y los Clientes (y sus clientes y afiliados); y
  - v) mitigar y corregir oportuna y adecuadamente los efectos de la Incidencia de Seguridad e implementar controles y procesos adicionales para reducir el riesgo de incidencias similares en el futuro, al mismo tiempo que se presta la debida consideración a cualquier comentario de Kyndryl sobre dichas mitigaciones y correcciones.
- (c) El Proveedor es responsable de todos los costes y gastos incurridos por el Proveedor en la investigación, la respuesta, la mitigación y la corrección de una Incidencia de Seguridad. Sujeto a la limitación de responsabilidad en el Acuerdo, el Proveedor también es responsable de todos los costes y gastos varios incurridos por Kyndryl, los afiliados de Kyndryl y los Clientes (y sus clientes y afiliados) en relación con la investigación, la respuesta, la mitigación y la corrección de la Incidencia de Seguridad. Los costes y gastos relacionados con la corrección de incidencias de seguridad pueden incluir los costes relacionados con detectar e investigar una incidencia de seguridad, determinar las responsabilidades en virtud de las leyes y las normativas, volver a cargar datos, corregir defectos de un producto (incluso a través del Código Fuente u otro desarrollo), contratar a terceros para asistencia con las actividades anteriores u otras actividades relevantes, y otros costes y gastos que sean necesarios para subsanar los efectos nocivos de la Incidencia de Seguridad.
- (d) En caso de una Incidencia de Seguridad que afecte a Datos Personales de Kyndryl, el Proveedor es responsable de los costes en los que incurra y reembolsará a Kyndryl los costes y gastos en los que incurra Kyndryl relacionados con:
- i) Notificar la Incidencia de Seguridad a los reguladores aplicables, otros organismos del gobierno y de autorregulación del sector relevantes, a los medios de comunicación (si así lo requiere la legislación aplicable), a los Interesados, a los Clientes y a otros;
  - ii) Establecer y mantener un centro de llamadas para responder a las preguntas de los Interesados sobre la Incidencia de Seguridad y sus consecuencias, durante un plazo de 1 año a partir de la fecha de notificación a dichos Interesados de la Incidencia de Seguridad, o un plazo superior, si así lo requiere ley de protección de datos aplicable. Kyndryl y el Proveedor trabajarán conjuntamente para crear las instrucciones y otros materiales que utilizará el personal del centro de llamadas para responder a las consultas relacionadas con los Datos Personales de Kyndryl; y
  - iii) Proporcionar servicios de protección contra la usurpación de identidad, de supervisión de crédito y de restauración de crédito durante un plazo de 2 años a partir de la fecha de notificación de la Incidencia de Seguridad a los Interesados afectados por la incidencia que decidan registrarse en dichos servicios, o un plazo superior, si así lo requiere la legislación aplicable.
- (e) El Proveedor no identificará, directa o indirectamente, a Kyndryl ante ningún tercero como afectado por una Incidencia de Seguridad, a menos que Kyndryl apruebe hacerlo por escrito o cuando lo requiera ley. El Proveedor notificará a Kyndryl por escrito antes de distribuir cualquier notificación legalmente requerida a un tercero que revele directa o indirectamente la identidad de Kyndryl.
- (f) El Proveedor también notificará de inmediato a Kyndryl cualquier amenaza real o inminente de violación de estos Términos o sus políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable en relación con la entrega de un Producto o los Servicios.

### 3.13. Relaciones con los proveedores

- (a) **Subcontratistas.** El Proveedor es responsable del cumplimiento de estos Términos incluso si utiliza un Subcontratista. El Proveedor obligará contractualmente a dichos Subcontratistas a proteger los Materiales de Kyndryl mediante términos no menos completos o estrictos que aquellos aplicables al Proveedor en los Términos. El Proveedor es responsable ante Kyndryl del rendimiento de cada Subcontratista.
- (b) **Control de calidad y Gestión de la seguridad.** El Proveedor realizará el control de calidad y la supervisión de la gestión de la seguridad del desarrollo de software subcontratado a un Subcontratista.
- (c) **Información precontractual.** El Proveedor declara y garantiza que toda información material proporcionada durante las conversaciones precontractuales con Kyndryl en relación con la privacidad, la seguridad y el gobierno de datos, ya sea de conformidad con estos Términos 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 de la seguridad y evaluación

- (a) **Verificación** El Proveedor mantendrá un registro auditable que demuestre el cumplimiento de estos Términos.
- (i) Kyndryl, por sí mismo o con un auditor externo, podrá, previo aviso por escrito al Proveedor con 30 días de antelación, verificar la conformidad del Proveedor con estos Términos, incluso acceder a cualquier Instalación o Instalaciones para tales fines, aunque Kyndryl no accederá a ningún centro de datos donde el Proveedor realice el Tratamiento de Datos de Kyndryl a menos que tenga un motivo de buena fe para creer que hacerlo proporcionaría información relevante. El Proveedor cooperará con la verificación de Kyndryl, incluso respondiendo oportuna y completamente a las solicitudes de información, ya sea a través de documentos, otros registros, entrevistas con el Personal pertinente del Proveedor o similares. El Proveedor puede ofrecer pruebas de su adhesión a un código de conducta aprobado o a una certificación del sector, o bien proporcionar información que demuestre el cumplimiento de estos Términos, para su consideración por parte de Kyndryl.
  - (ii) Una verificación no se producirá más de una vez en cualquier periodo de 12 meses, a menos que: (A) Kyndryl esté validando la corrección por parte del Proveedor de problemas derivados de una verificación anterior durante el período de 12 meses o (B) se haya producido una Incidencia de seguridad y Kyndryl desee verificar la conformidad con las obligaciones pertinentes a la incidencia. En cualquier caso, Kyndryl proporcionará el mismo aviso por escrito con 30 días de anticipación que se ha especificado en el párrafo (i) anterior, pero la urgencia de abordar una Incidencia de Seguridad puede requerir que Kyndryl realice una verificación con un aviso por escrito de menos de 30 días.
  - (iii) Un regulador o bien, cuando la legislación lo permita, otro Responsable puede ejercer los mismos derechos que Kyndryl en los párrafos (ii) y (iii), entendiéndose que un regulador puede ejercer cualquier derecho adicional que tenga en virtud de la ley.
  - (iv) Si Kyndryl tiene motivos razonables para concluir que el Proveedor incumple alguno de estos Términos (tanto si dichos motivos se derivan de una verificación en virtud de estos Términos o de otro modo), el Proveedor subsanará de inmediato dicho incumplimiento.
  - (v) Esta Sección se aplicará adicionalmente a 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 cuestionar si alguno de los Servicios o Productos puede haber contribuido, contribuye o contribuirá a algún problema de ciberseguridad, el Proveedor cooperará razonablemente con cualquier investigación de Kyndryl relativa a dicho problema, lo que incluye responder puntual y completamente a las solicitudes de información, ya sea mediante documentos, otros registros, entrevistas con el personal pertinente del Proveedor o similares.
- (c) **Cumplimiento de la seguridad.** El Proveedor obtendrá (i) una certificación de conformidad con ISO 27001, de una empresa auditora pública independiente, (ii) un informe de una empresa auditora pública independiente que demuestre que ha revisado los sistemas, controles y operaciones del Proveedor de acuerdo con un SOC 2 Tipo 2 que, como mínimo, incluya los Principios de Servicio de Confianza de Seguridad (también denominados Criterios Comunes), Disponibilidad y Confidencialidad y (iii) un informe de una empresa auditora pública independiente que demuestre que ha revisado 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 la orientación futura relacionada con SSAE18 emitida por la AICPA, IAASB, la Securities and Exchange Commission o la Public Company Accounting Oversight Board (PCAOB). Previa solicitud, el Proveedor proporcionará de inmediato a Kyndryl una copia de cada certificado e informe que el Proveedor está 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 Producto individual, el Proveedor cumplimentará de manera precisa y oportuna (en un plazo no superior a 14 Días) un cuestionario para verificar el cumplimiento del Proveedor con sus obligaciones en materia de ciberseguridad y gobierno de datos en virtud del Acuerdo y estos Términos ("**Evaluación del Cumplimiento**"). Si, después de finalización la Evaluación de Cumplimiento, Kyndryl determina razonablemente que las prácticas y los procedimientos de seguridad y gobierno de datos del Proveedor no cumplen con las obligaciones del Proveedor, Kyndryl notificará al Proveedor sobre las deficiencias. Si el Proveedor está de acuerdo con la evaluación de las deficiencias realizada por Kyndryl, el Proveedor, sin retraso injustificado: (i) corregirá dichas deficiencias a su propio coste en un periodo de tiempo acordado con Kyndryl conforme a 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 las deficiencias calificadas como de gravedad alta o crítica en el periodo de tiempo acordado, Kyndryl tiene el derecho de rescindir el Documento de Transacción aplicable o el Acuerdo por incumplimiento significativo inmediatamente después de la notificación al Proveedor. Kyndryl no revelará la documentación a ningún tercero que no sea sus propios auditores sin autorización por escrito del Proveedor. Si el Proveedor no está de acuerdo con la evaluación de las deficiencias realizada por Kyndryl, el Proveedor proporcionará sin demora a Kyndryl una explicación por escrito detallando sus razones y, si Kyndryl no acepta las razones del Proveedor, las partes escalarán a su respectivo Director de Privacidad, Director de Seguridad de la Información o un ejecutivo con un ámbito de actuación y autoridad similares para una resolución oportuna. Si las deficiencias se deben al uso de los Servicios por parte de Kyndryl, el Proveedor brindará el soporte técnico razonable para prestar asistencia a Kyndryl con la utilización apropiada de los Servicios a fin de 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 garantizará que sus empleados con acceso cumplan con 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 dichos empleados accederán a los Sistemas corporativos a través de Dispositivos proporcionados por el Proveedor o por Kyndryl.
- (c) Los empleados del Proveedor solo podrán acceder a los Sistemas Corporativos y solo podrán utilizar los Dispositivos que Kyndryl autorice para dicho acceso, para prestar 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 puede acceder a través de un Sistema Corporativo sin la aprobación previa por escrito de Kyndryl (y nunca copiarán ningún Material de Kyndryl en un dispositivo de almacenamiento portátil, como un USB, un disco duro externo u otros artículos similares).
- (e) Previa solicitud, el Proveedor confirmará, por nombre de empleado, los Sistemas Corporativos específicos a los que sus empleados están autorizados a acceder, y a los que han accedido, durante cualquier periodo de tiempo que Kyndryl identifique.
- (f) El Proveedor avisará a Kyndryl en un plazo de veinticuatro (24) horas después de que cualquier empleado del Proveedor con acceso a cualquier Sistema Corporativo deje de: (i) ser empleado del Proveedor o (ii) trabajar en actividades que requieran dicho acceso. El Proveedor trabajará con Kyndryl para garantizar que el acceso de dichos empleados o exempleados se revoque de inmediato.
- (g) El Proveedor informará inmediatamente a Kyndryl de cualquier incidencia de seguridad real o supuesta (como la pérdida de un Dispositivo del Proveedor o de Kyndryl o el acceso no autorizado a un Dispositivo o a datos, materiales u otra información de cualquier tipo) y cooperará con Kyndryl en la investigación de tales incidencias.
- (h) El Proveedor no permitirá que ningún agente, contratista independiente o empleado subcontratista acceda a ningún Sistema Corporativo, sin la autorización previa por escrito de Kyndryl; si Kyndryl proporciona esa autorización, el Proveedor obligará contractualmente a esas personas y sus empleadores a cumplir con los requisitos de este Artículo como si esas personas fueran empleados del Proveedor, y será responsable ante Kyndryl de todas las acciones y omisiones de dicha persona o empleador con respecto al acceso a dicho Sistema Corporativo.
- (i) Kyndryl puede revocar el acceso a los Sistemas Corporativos en cualquier momento, de cualquier empleado del Proveedor o de todo el Personal del Proveedor, sin necesidad de avisar previamente al Proveedor ni a ningún empleado del Proveedor ni a otros, si Kyndryl lo considera necesario para la protección de Kyndryl.
- (j) Los derechos de Kyndryl no están bloqueados, disminuidos o restringidos en modo alguno por ninguna disposición del Documento de Transacción, el acuerdo base asociado entre las partes o cualquier otro acuerdo entre las partes, incluida cualquier disposición que pueda requerir que los datos, materiales u otra información de cualquier tipo se alojen solo en una ubicación o ubicaciones seleccionadas o que pueda requerir que solo las personas de una ubicación o ubicaciones seleccionadas accedan a dichos datos, materiales u otra información.

#### **4.2. Software del dispositivo**

- (a) El Proveedor ordenará a su Personal la instalación oportuna de software en los Dispositivos de Kyndryl y del Proveedor que Kyndryl requiera para facilitar el acceso seguro a los Sistemas Corporativos. Ni el Proveedor ni su Personal interferirán en las operaciones de ese software ni en las características de seguridad que el software habilita.
- (b) El Proveedor y su Personal cumplirán con las normas de configuración de los Dispositivos de Kyndryl y del Proveedor que establezca Kyndryl y colaborarán con Kyndryl para ayudar a garantizar que el software funcione según lo previsto por Kyndryl. Por ejemplo, el Proveedor no anulará el software de bloqueo de sitios web ni las funciones de aplicación automática de parches.
- (c) El Personal del Proveedor no puede compartir nombres de usuario, contraseñas ni información similar de los Dispositivos de Kyndryl y 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 aquellos Dispositivos que Kyndryl apruebe y actualizará a una nueva versión de ese sistema operativo o a 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 proporcionar servicios a cualquier otra persona o entidad, o para acceder a los sistemas de TI, redes, aplicaciones, sitios web, herramientas de correo electrónico, herramientas de colaboración o similares de cualquier Proveedor o de terceros en relación con los Servicios. Los empleados del Proveedor no pueden utilizar los Dispositivos de Kyndryl por motivos personales (por ejemplo, los empleados del Proveedor no pueden almacenar archivos personales como música, vídeos, imágenes u otros elementos similares en dichos Dispositivos de Kyndryl, ni pueden utilizar 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 utilicen para acceder a los Sistemas corporativos.
- (b) Kyndryl tiene los derechos incondicionales para supervisar los Dispositivos de Kyndryl y los Sistemas corporativos y de subsanar posibles intrusiones y otras amenazas de ciberseguridad de cualquier forma, desde cualquier lugar y usando cualquier medio que Kyndryl crea necesario o apropiado, sin previo aviso al Proveedor ni a ningún empleado del Proveedor u otros. Como ejemplos de tales derechos, Kyndryl puede, en cualquier momento, (i) realizar pruebas de seguridad en cualquier Dispositivo de Kyndryl, (ii) supervisar, recuperar a través de medios técnicos o de otro tipo y revisar las comunicaciones (incluidos los correos electrónicos de cualquier cuenta de correo electrónico en los Dispositivos de Kyndryl), registros, archivos y otros elementos almacenados en cualquier Dispositivo de Kyndryl o transmitidos a través de cualquier Sistema corporativo, y (iii) obtener una imagen forense completa de cualquier Dispositivo de Kyndryl. Si Kyndryl necesita la cooperación del Proveedor para ejercer sus derechos, el Proveedor satisfará completa y oportunamente las solicitudes de Kyndryl en relación con dicha cooperación (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 los detalles de conexión al nivel del sistema, participar en medidas de respuesta a incidencias en cualquier Dispositivo 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 mantendrá la propiedad de todos los Dispositivos de Kyndryl y el Proveedor asumirá el riesgo de pérdida de los Dispositivos de Kyndryl, incluso debido a robo, vandalismo o negligencia. El Proveedor no realizará ni permitirá ninguna modificación en los Dispositivos de Kyndryl sin la autorización previa 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 del Dispositivo, así como cambios físicos, mecánicos o de diseño eléctrico.
- (d) El Proveedor devolverá todos los Dispositivos de Kyndryl en un plazo de 5 días hábiles tras finalizar la necesidad de que esos Dispositivos brinden 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 conservar ninguna copia, siguiendo los siguientes estándares 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 se le entregaron, aparte del desgaste razonable, a su propio coste, hasta el lugar que Kyndryl indique. El incumplimiento por parte del Proveedor de cualquier obligación en este párrafo (d) constituye un incumplimiento significativo del Documento de transacción, del acuerdo base asociado y de cualquier acuerdo relacionado entre las partes, entendiéndose que un acuerdo está "relacionado" si el acceso a cualquier Sistema corporativo facilita las tareas del Proveedor u otras actividades en virtud de ese acuerdo.
- (e) Kyndryl proporcionará soporte para los Dispositivos de Kyndryl (incluida la inspección del Dispositivo y el mantenimiento preventivo y correctivo). El Proveedor informará inmediatamente a Kyndryl de la necesidad de un servicio de reparación.
- (f) Para los programas de software de los que Kyndryl es propietario o tiene derecho a asignar licencias, Kyndryl otorga al Proveedor un derecho temporal de uso, almacenamiento y realización de copias suficientes para respaldar el uso autorizado de los Dispositivos de Kyndryl. El Proveedor no puede transferir programas a nadie, hacer copias de la información de licencia del software, ni desensamblar, descompilar, someter a ingeniería inversa ni traducir cualquier programa a menos que esté permitido expresamente por la legislación aplicable sin posibilidad de renuncia por contrato.

## Article V. DEFINICIONES

Los términos "Servicios" y "Productos" se definen del mismo modo en el Acuerdo de Relación con el Proveedor o un Acuerdo equivalente o un Documento de Transacción; pero si no es así, "**Servicios**" hace referencia a cualquier tarea de alojamiento, consultoría, instalación, personalización, mantenimiento, soporte, aumento de personal, trabajo comercial, técnico o de otro tipo que el Proveedor realice para Kyndryl, como se especifica en el Documento de Transacción, y "**Productos**" hace referencia a 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** hace referencia a 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** hace referencia a un sistema basado en máquinas que está diseñado para operar 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. **Información de Contacto Comercial ("BCI", por sus siglas en inglés)** hace referencia a los Datos Personales utilizados para contactar con una persona, identificarla o autenticarla de forma profesional o comercial para fines únicamente administrativos y de gestión de contrato (por ejemplo, facturación y gestión de cuentas, cálculo de incentivos de partner, informes internos y modelos de negocio tales como la previsión y la planificación de ingresos y de capacidad). Por lo general, la BCI incluye el nombre de una persona, su dirección de correo electrónico corporativa, dirección física, número de teléfono o atributos similares. Por ejemplo, los nombres y direcciones de correo electrónico utilizados para contactar con el Personal del Proveedor para los servicios de soporte son BCI; sin embargo, los nombres y direcciones de correo electrónico incluidos en los datos de diagnóstico son Datos Personales de Kyndryl.
- 5.4. **Servicio en la Nube** hace referencia a cualquier oferta "como servicio" alojada o gestionada por el Proveedor, incluidas las ofertas de "software como servicio", "plataforma como servicio" e "infraestructura como servicio".
- 5.5. **Responsable** hace referencia a la persona física o jurídica, la autoridad pública, la agencia u otro organismo que, individualmente o junto con otros, determina los fines y los medios del Tratamiento de Datos Personales.
- 5.6. **Sistema Corporativo** hace referencia a un sistema de TI, plataforma, aplicación, red o similar que Kyndryl utilice para su negocio, incluidos aquellos ubicados o accesibles a través de la intranet de Kyndryl, Internet u otros.
- 5.7. **Cliente** hace referencia a un cliente de Kyndryl.
- 5.8. **Importador de Datos** hace referencia a un Encargado o un Subencargado que no está establecido en un País Adecuado.
- 5.9. **Interesado** hace referencia a una persona física que puede ser identificada, directa o indirectamente.
- 5.10. **Día o Días** hace referencia a días naturales, a menos que se designen días "hábiles".
- 5.11. **Dispositivo** se refiere a una estación de trabajo, portátil, tableta, teléfono inteligente o asistente digital personal proporcionado por Kyndryl o el Proveedor.
- 5.12. **Instalaciones** hace referencia a una ubicación física donde el Proveedor aloja, accede a o procesa de otro modo los Productos o Materiales de Kyndryl.
- 5.13. **Prácticas Estándares del Sector** hace referencia a aquellas prácticas recomendadas o requeridas por el Instituto Nacional de Estándares y Tecnología ("NIST") o la Organización Internacional de Estándares ("ISO"), o a cualquier otro organismo u organización de reputación y sofisticación similares.
- 5.14. **Datos de Kyndryl** hace referencia a todos y cada uno de los datos, archivos, materiales, texto, audio, vídeo, imágenes u otros datos, incluidos los Datos Personales de Kyndryl, la BCI de Kyndryl y los Datos no Personales de Kyndryl, que se proporcionan al Proveedor o a los que se facilita el acceso (incluido, entre otros, a través de un Servicio en la Nube) en relación con la entrega de los Servicios o un Producto, independientemente de si es Kyndryl, el Personal de Kyndryl, un Cliente, un empleado del Cliente o un contratista, o cualquier otra persona o entidad quien los proporciona o facilita el acceso.
- 5.15. **Materiales de Kyndryl** hace referencia a todos y cada uno de los Datos de Kyndryl y la Tecnología de Kyndryl.
- 5.16. **Datos Personales de Kyndryl** hace referencia a los Datos Personales, excluyendo la BCI de Kyndryl, que Kyndryl proporciona o pone a disposición del Proveedor para la entrega de los Servicios o Productos. Los Datos Personales de Kyndryl incluyen los Datos Personales que Kyndryl controla y los Datos Personales de los que Kyndryl realiza el Tratamiento en nombre de Otros Responsables.
- 5.17. **Tecnología de Kyndryl** hace referencia al Código Fuente de Kyndryl, otros códigos, lenguajes descriptivos, firmware, software, herramientas, diseños, esquemas, representaciones gráficas, claves incorporadas,

- certificados y otra información, materiales, activos, documentos y tecnología que Kyndryl ha licenciado directa o indirectamente o ha puesto a disposición del Proveedor por cualquier otro medio en relación con el Documento de Transacción o un Acuerdo.
- 5.18. **País No Adecuado** hace referencia a un país que no se considera adecuado de conformidad con las leyes de protección de datos aplicables o una decisión de un regulador competente.
  - 5.19. **Otro Responsable** hace referencia a cualquier entidad distinta de Kyndryl que sea Responsable de los Datos de Kyndryl, como un afiliado de Kyndryl, un Cliente o un afiliado de un Cliente.
  - 5.20. **Software Local** hace referencia al software proporcionado por el Proveedor como un Producto 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** hace referencia a cualquier información relacionada con un Interesado y cualquier otra información considerada como "datos personales" o similar en virtud de cualquier ley de protección de datos.
  - 5.22. **Personal** hace referencia a 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 de las partes por un subcontratista.
  - 5.23. **Tratamiento, Tratar o Realizar el Tratamiento** hace referencia a cualquier operación o conjunto de operaciones realizadas sobre los Datos de Kyndryl, incluido el almacenamiento, el uso, el acceso y la lectura.
  - 5.24. **Encargado** hace referencia a una persona jurídica que realiza el Tratamiento de Datos Personales en nombre de un Responsable e incluye "proveedor de servicio" o términos sustancialmente similares en virtud de cualquier ley de protección de datos.
  - 5.25. **Incidencia de Seguridad** hace referencia a (a) una suceso que, de forma real o inminente, pone en peligro la confidencialidad, la integridad o la disponibilidad de cualquier Material de Kyndryl o un sistema de información utilizado por el Proveedor o sus Subcontratistas para proporcionar los Servicios o Productos, (b) una violación de la seguridad que causa la destrucción accidental o ilícita, la pérdida, la alteración, la revelación no autorizada de, o el acceso a, Datos de Kyndryl transmitidos, almacenados o Tratados de otro modo, o (c) el acceso a, o la utilización sin autorización de, Código Fuente utilizado por el Proveedor o sus Subcontratistas en la entrega de los Servicios o un Producto o en relación con este hecho.
  - 5.26. **Vender** (o **Venta**) hace referencia a alquilar, publicar, divulgar, difundir, poner a disposición, transferir o comunicar de otro modo, de forma oral, por escrito o por medios electrónicos u otros, datos a cambio de una compensación económica u otra contraprestación valiosa.
  - 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")** hace referencia a las cláusulas contractuales exigidas por las leyes de protección de datos aplicables para la transferencia de Datos personales a Encargados que no estén establecidos en un País Adecuado.
  - 5.29. **Código Fuente** hace referencia a código de programación legible por humanos o a código que se puede convertir a un formato legible por humanos que los desarrolladores utilizan en la creación, el desarrollo o el mantenimiento de un producto, pero que no se hace público en el transcurso normal de la distribución o el uso comercial del producto.
  - 5.30. **Subencargado** hace referencia a cualquier Subcontratista del Proveedor, incluido un afiliado del Proveedor, que realice el Tratamiento de Datos Personales de Kyndryl.
  - 5.31. **Autoridad de control** hace referencia a un organismo público independiente responsable de supervisar la aplicación de las leyes de protección de datos dentro de una región o un país específico.