Artículo I, Información Profesional de Contacto

Este artículo se aplica si el Proveedor o Kyndryl tratan la BCI de la otra parte.

1.1 Kyndryl y el Proveedor pueden tratar la BCI de la otra parte donde hagan negocios en relación con la prestación de Servicios y Entregable por parte del Proveedor.

1.2 Ninguna parte:

a) usará ni revelará la BCI de la otra parte para ningún otro propósito (para mayor claridad, ninguna de las partes venderá la BCI de la otra parte o usará o revelará la BCI de la otra parte con ninguna finalidad empresarial sin el consentimiento previo por escrito de la otra parte y, cuando sea necesario, el consentimiento previo por escrito de los Interesados afectados), y

b) eliminará, modificará, corregirá, devolverá, proporcionará información sobre el Tratamiento, restringirá el Tratamiento o realizará ninguna otra acción razonablemente solicitada con respecto a la BCI de la otra parte, puntualmente a solicitud por escrito de la otra parte.

1.3 Las partes no establecen una relación conjunta de Responsable del Tratamiento con respecto a la BCI de cada una de ellas y ninguna cláusula del Documento Transaccional se considerará o interpretará como una indicación de intención de establecer una relación conjunta de Responsable del Tratamiento.

1.4 La Declaración de Privacidad de Kyndryl en https://www.kyndryl.com/Privacy contiene detalles adicionales sobre el Tratamiento de BCI por parte de Kyndryl.

1.5 Las partes han implementado y mantendrán medidas de seguridad técnicas y organizativas para proteger la BCI de la otra parte frente a pérdida, destrucción, alteración, revelación accidental o no autorizada, acceso accidental o no autorizado y Tratamiento ilegal.

1.6 El Proveedor avisará a Kyndryl inmediatamente (y en ningún caso más tarde de 48 horas) tras conocer cualquier brecha de seguridad que involucre la BCI de Kyndryl. El proveedor proporcionará dicha notificación a cyber.incidents@kyndryl.com. El Proveedor suministrará a Kyndryl la información razonablemente solicitada acerca de la infracción y del estado de las actividades de corrección y restauración llevadas a cabo por cualquier Proveedor. A modo de ejemplo, la información solicitada razonablemente puede incluir registros que demuestren acceso privilegiado, administrativo y de otro tipo a Dispositivos, sistemas o aplicaciones, imágenes forenses de Dispositivos, sistemas o aplicaciones y otros elementos similares, en la medida que sean relevantes con la infracción o las actividades de reparación y restauración del Proveedor.

1.7 Cuando el Proveedor solo trate la BCI de Kyndryl y no tenga acceso a ningún otro dato o material de ningún tipo ni a ningún Sistema Corporativo de Kyndryl, este Artículo y el Artículo X (Cooperación, Verificación y Remediación) son los únicos artículos que se aplican al Tratamiento.

Artículo II, Medidas Técnicas y Organizativas, Seguridad de los Datos

Este Artículo se aplica si el Proveedor trata datos de Kyndryl, que no sean BCI de Kyndryl. El Proveedor cumplirá los requisitos de este Artículo proporcionando todos los Servicios y Entregables, y al hacerlo protegerá los Datos de Kyndryl contra pérdida, destrucción, alteración, revelación accidental o no autorizada, acceso accidental o no autorizado, y formas ilegales de Tratamiento. Los requisitos de este Artículo se extienden a todas las aplicaciones, plataformas e infraestructura de TI que el Proveedor opera o administra para proporcionar Entregables y Servicios, incluidos todos los entornos de desarrollo, pruebas, alojamiento, soporte, operaciones y centros de datos.

1. Uso de Datos

1.1. El Proveedor no puede agregar a los Datos de Kyndryl ni incluir con los Datos de Kyndryl ninguna otra información o datos, incluidos Datos Personales, sin el consentimiento previo por escrito de Kyndryl, y el Proveedor no puede usar los Datos de Kyndryl de ninguna forma, agregada o de otro modo, para ningún otro fin que no sea prestar Servicios y Entregables (a modo de ejemplo, al Proveedor no se le permite usar o reutilizar los Datos de Kyndryl para evaluar la eficacia o los medios para mejorar las ofertas del Proveedor, para la investigación y el desarrollo para crear nuevas ofertas, o para generar informes sobre las ofertas del Proveedor). A menos que se permita expresamente en el Documento Transaccional, el Proveedor tiene prohibido Vender Datos de Kyndryl.

1.2. El Proveedor no incorporará ninguna tecnología de seguimiento web en los Entregables o como parte de los Servicios (estas tecnologías incluyen HTML5, almacenamiento local, etiquetas o tokens de terceros y balizas web) a menos que esté expresamente permitido en el Documento Transaccional.

2. Confidencialidad y Solicitudes de Terceros

2.1. El Proveedor no revelará los Datos de Kyndryl a ningún tercero, a menos que Kyndryl lo autorice previamente por escrito. Si una autoridad pública, 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 una revelación de los Datos de Kyndryl, el Proveedor notificará a Kyndryl por escrito dicha demanda o requisito y brindará a Kyndryl una oportunidad razonable para impugnar cualquier revelación (si la ley prohíbe la notificación, el Proveedor tomará las medidas que razonablemente considere apropiadas para impugnar la prohibición y revelación de los Datos de Kyndryl a través de acciones judiciales u otros medios).

2.2. El Proveedor garantiza a Kyndryl que: (a) solo sus empleados que necesiten acceso a los Datos de Kyndryl para prestar Servicios o Entregables tendrán ese acceso, y posteriormente solo en la medida necesaria para proporcionar los Servicios y Entregables; y (b) ha vinculado a sus empleados a obligaciones de confidencialidad que requieren que los empleados solo usen y revelen Datos de Kyndryl según lo permitido en estas Condiciones.

3. Devolución o Eliminación de Datos de Kyndryl

3.1. El Proveedor, a elección de Kyndryl, eliminará o devolverá los Datos de Kyndryl a Kyndryl al terminar o vencer el Documento Transaccional, o con anterioridad a petición de Kyndryl. Si Kyndryl requiere la eliminación, el Proveedor, de acuerdo con las Prácticas Recomendadas del Sector, hará que los datos sean ilegibles y no puedan reensamblarse o reconstruirse, y certificará la eliminación a Kyndryl. Si Kyndryl requiere la devolución de los Datos de Kyndryl, el Proveedor lo hará bajo una programación razonable de Kyndryl y según las instrucciones escritas razonables de Kyndryl.

Artículo III, Privacidad

Este Artículo se aplica si el Proveedor trata Datos Personales de Kyndryl.

1. Tratamiento

1.1 Kyndryl designa al Proveedor como Encargado del Tratamiento para tratar los Datos Personales de Kyndryl con el único objetivo de proporcionar los Entregables y los Servicios de acuerdo con las instrucciones de Kyndryl, incluidas las contenidas en estas Condiciones, el Documento Transaccional y el acuerdo base asociado entre las partes. Si el Proveedor no acepta una instrucción, Kyndryl puede rescindir la parte afectada de los Servicios mediante 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 temporal que requiera la legislación pertinente.

1.2 El Proveedor cumplirá toda la legislación de protección de datos aplicable a los Servicios y Entregables.

1.3 Un Suplemento del Documento Transaccional, o el Documento Transaccional en sí, establece lo siguiente con respecto a los Datos de Kyndryl:

(a) categorías de Interesados;
(b) tipos de Datos Personales de Kyndryl;
(c) acciones de datos y actividades de Tratamiento;
(d) duración y frecuencia de Tratamiento; y
(e) una lista de Subencargados del Tratamiento.

2. Medidas Técnicas y Organizativas

2.1 El Proveedor implementará y mantendrá las medidas técnicas y organizativas establecidas en el Artículo II (Medidas Técnicas y Organizativas, Seguridad de los Datos) y el Artículo VIII (Medidas Técnicas y Organizativas, Seguridad General), y con ello garantizará un nivel de seguridad adecuado al riesgo de sus Servicios y Entregables presentes. El Proveedor certifica y comprende las restricciones del Artículo II, este Artículo III y el Artículo VIII, y las cumplirá.

3. Solicitudes y Derechos de los Interesados

3.1 El Proveedor notificará a Kyndryl de inmediato (bajo una programación que permita a Kyndryl y a cualquier otro Responsable del Tratamiento cumplir sus obligaciones legales) 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 dirigir de inmediato a un Interesado que realice dicha solicitud 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.

3.2 Si Kyndryl está obligada a proporcionar información sobre los Datos Personales de Kyndryl a otros Responsables del Tratamiento 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, bajo una programación que permita a Kyndryl responder oportunamente a dichos otros Responsables del Tratamiento o terceros.

4. Subencargados del Tratamiento

4.1 El Proveedor proporcionará a Kyndryl un aviso por escrito antes de incluir un nuevo Subencargado del Tratamiento o de ampliar el alcance del Tratamiento por parte de un Subencargado del Tratamiento existente, y con dicho aviso por escrito identificará el nombre del Subencargado del Tratamiento y describirá el alcance nuevo o ampliado del Tratamiento. Kyndryl puede oponerse a cualquier nuevo Subencargado del Tratamiento o la ampliación en el alcance del mismo por motivos razonables en

cualquier momento, y si lo hace, las partes trabajarán juntas de buena fe para abordar la objeción de Kyndryl. Sujeto al derecho de Kyndryl de oponerse en cualquier momento, el Proveedor puede nombrar el nuevo Subencargado del Tratamiento o ampliar el alcance del Tratamiento del Subencargado del Tratamiento existente si Kyndryl no ha presentado ninguna objeción dentro del plazo de 30 días posterior a la fecha del aviso por escrito del Proveedor.

4.2 El Proveedor impondrá las obligaciones de protección de datos, seguridad y certificación establecidas en estas Condiciones sobre cada Subencargado del Tratamiento aprobado antes de que un Subencargado del Tratamiento trate Datos de Kyndryl. El Proveedor es plenamente responsable ante Kyndryl por el cumplimiento de las obligaciones de cada Subencargado del Tratamiento.

5. Tratamiento de Datos Transfronterizo

Según su uso a continuación:

País Adecuado: país que proporciona un nivel adecuado de protección de datos respecto a la transferencia correspondiente de conformidad con la legislación de protección de datos o las decisiones de los reguladores aplicables.

Importador de Datos: Encargado del Tratamiento o Subencargado del Tratamiento que no está establecido en un País Adecuado.

Cláusulas Contractuales Tipo de la UE ("SCC de la UE"): Cláusulas Contractuales Tipo de la UE (Decisión 2021/914 de la Comisión) con las cláusulas opcionales aplicadas, excepto la opción 1 de la Cláusula 9(a) y la opción 2 de la Cláusula 17, tal como se ha publicado oficialmente en https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Cláusulas Contractuales Tipo de Serbia ("SCC de Serbia") Cláusulas Contractuales Tipo de Serbia según su adopción por parte del "Comisionado para la Información de Importancia Pública y la Protección de Datos Personales de Serbia", publicadas en https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx .

Cláusulas Contractuales Tipo ("**SCC**"): cláusulas contractuales requeridas por la legislación de protección de datos aplicable para la transferencia de Datos Personales a los Encargados del Tratamiento que no están establecidos en Países Adecuados.

Anexo sobre las Transferencias Internacionales de Datos del Reino Unido a las Cláusulas Contractuales Tipo de la Comisión de la UE ("Anexo del Reino Unido") hace referencia al Anexo sobre Transferencias Internacionales de Datos del Reino Unido a las Cláusulas Contractuales Tipo de la Comisión de la UE tal como se ha publicado oficialmente en la página https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/.

El anexo suizo a las Cláusulas contractuales tipo de la Comisión Europea (en adelante, el «Anexo suizo») hace referencia a las Cláusulas contractuales tipo de la Comisión Europea que se aplican en conformidad con la decisión de la Autoridad Suiza de Protección de Datos (**«FDPIC»**) y en conformidad con la Ley Federal Suiza sobre Protección de Datos (**«FADP»**).

5.1 El Proveedor no transferirá ni revelará (incluso mediante acceso remoto) ningún Dato Personal de Kyndryl a nivel transfronterizo sin el consentimiento previo por escrito de Kyndryl. Si Kyndryl proporciona dicho consentimiento, las partes cooperarán para garantizar el cumplimiento de la legislación de protección de datos aplicable. Si esta legislación requiere las SCC, el Proveedor incorporará de inmediato las SCC a solicitud de Kyndryl.

5.2 En relación con las SCC de la UE:

(a) Si el Proveedor no está establecido en un País Adecuado: por el presente documento, el Proveedor que incorpora las SCC de la UE como Importador de Datos con Kyndryl y el Proveedor firmarán acuerdos por escrito con cada Subencargado del Tratamiento aprobado, de acuerdo con la Cláusula 9 de las SCC de la UE, y proporcionará a Kyndryl copias de esos acuerdos, a petición.

(i) El Módulo 1 de las SCC de la UE no se aplica a menos que las partes lo acuerden por escrito.

(ii) El Módulo 2 de las SCC de la UE se aplica cuando Kyndryl es un Responsable del Tratamiento y el Módulo 3 se aplica cuando Kyndryl es un Encargado del Tratamiento. De acuerdo con la Cláusula 13 de las SCC de la UE, cuando se aplican los Módulos 2 o 3, las partes acuerdan que (1) las SCC de la UE se regirán por la legislación del estado miembro de la UE donde se encuentre la autoridad de supervisión competente y (2) cualquier disputa que surja de las SCC de la UE será en los tribunales del estado miembro de la UE donde se encuentre la autoridad de supervisión. Si dicha legislación en (1) no permite derechos de beneficiario de terceros, las SCC de la UE se regirán por la legislación de los Países Bajos y cualquier disputa que surja de las SCC de la UE bajo (2) será resuelta por el tribunal de Ámsterdam en los Países Bajos.

(B) Si el Proveedor está establecido en el Espacio Económico Europeo e Kyndryl es un Responsable del Tratamiento que no está sujeto al Reglamento General de Protección de Datos 2016/679, se aplica el Módulo 4 de las SCC de la UE, y el Proveedor incorpora las SCC de la UE como exportador de datos con Kyndryl. Si se aplica el Módulo 4 de las SCC de la UE, las partes acuerdan que las SCC de la UE se regirán por la legislación de los Países Bajos y cualquier disputa que surja de las SCC de la UE será resuelta por el tribunal de Ámsterdam en los Países Bajos.

(C) Si Otros Responsables del Tratamiento, como Clientes o filiales, solicitan ser parte de las SCC de la UE de conformidad con la 'cláusula de acoplamiento' en la Cláusula 7, por el presente documento el Proveedor acepta dicha solicitud.

(D) Las Medidas Técnicas y Organizativas necesarias para completar el Anexo II de las SCC de la UE se pueden encontrar en estas Condiciones, el Documento Transaccional y el acuerdo base asociado entre las partes.

(e) En caso de conflicto entre las SCC de la UE y estas Condiciones, prevalecerán las SCC de la UE.

5.3 En relación con las SCC del Reino Unido:

(a) Si el Proveedor no está establecido en un País Adecuado: (i) por el presente documento, el Proveedor incorpora las SCC del Reino Unido con Kyndryl actuando en nombre del Proveedor como Importador de Datos; y (ii) el Proveedor firmará acuerdos por escrito con cada Subencargado del Tratamiento aprobado que sea un Importador de datos, de conformidad con la Cláusula 11 de las SCC del Reino Unido, y proporcionará a Kyndryl copias de dichos acuerdos, a petición.

(b) Si el Proveedor está establecido en un País Adecuado, por el presente documento el Proveedor incorpora las SCC del Reino Unido con Kyndryl actuando en nombre de cada Subencargado del Tratamiento que sea un Importador de Datos. Si el Proveedor no puede hacerlo para ningún Subencargado del Tratamiento, el Proveedor proporcionará a Kyndryl las SCC del Reino Unido firmadas por el Subencargado del Tratamiento para la posterior firma de Kyndryl antes de permitir que el Subencargado del Tratamiento trate los Datos Personales de Kyndryl.

(c) Las SCC del Reino Unido entre Kyndryl y el Proveedor servirán como SCC del Reino Unido entre un Responsable del Tratamiento y un Encargado del Tratamiento o como acuerdo por escrito consecutivo entre el "Importador de datos" y el "Subencargado del Tratamiento" de conformidad con la Cláusula 11 de las SCC del Reino Unido, según lo exija la realidad. En caso de conflicto entre las SCC del Reino Unido y estas Condiciones, prevalecerán las SCC del Reino Unido.

(d) Otros Responsables del Tratamiento, como Clientes o afiliados, pueden solicitar ser 'exportadores de datos' adicionales. El Proveedor acepta en su propio nombre y en nombre de sus Subencargados del Tratamiento cualquier solicitud de este tipo. Kyndryl informará al Proveedor acerca de cualquier posible "exportador de datos" adicional y, a su vez, el Proveedor informará a sus Subencargados del Tratamiento que son Importadores de Datos de los "exportadores de datos" adicionales.

5.4 Acerca de los Anexos del Reino Unido:

a) Si el Proveedor no está establecido en un País Adecuado: (i) el Proveedor firma los Anexos del Reino Unido con Kyndryl como Importador para que se añadan a las Cláusulas Contractuales Tipo (SCCs) de la UE establecidas anteriormente (según sea aplicable, en función de las circunstancias de las actividades del tratamiento); y (ii) el Proveedor formalizará acuerdos por escrito con cada uno de los Subencargados aprobados y proporcionará a Kyndryl copias de estos acuerdos cuando se soliciten.

b) Si el Proveedor está establecido en un País Adecuado, y Kyndryl es un Responsable no sujeto al Reglamento General de Protección de Datos del Reino Unido (según se ha incorporado en la legislación del Reino Unido bajo a Ley sobre (la retirada de) la Unión Europea de 2018 (European Union (Withdrawal) Act 2018)), el Proveedor, por el presente documento, firma los Anexos como Exportador con Kyndryl para que se añadan a las SCCs de la UE establecidas en el Apartado 5.2(b) anterior.

c) Si otros Responsables del tratamiento de datos como, por ejemplo, Clientes o filiales, solicitan ser parte de los Anexos del Reino Unido, el Proveedor aceptará ese tipo de solicitudes.

d) La Información del Apéndice (tal como está establecida en la Tabla 3) en los Anexos del Reino Unido se puede encontrar en las SCCs de la UE aplicables, estas Condiciones, el propio Documento Transaccional y el acuerdo base asociado entre las partes. Ni Kyndryl ni el Proveedor pueden finalizar los Anexos del Reino Unido cuando estos cambien.

e) En caso de conflicto entre los Anexos del Reino Unido y estas Condiciones, los Anexos del Reino Unido prevalecerán.

5.5 Con respecto a las SCC de Serbia:

(a) Si el Proveedor no está establecido en un País Adecuado: (i) por el presente documento, el Proveedor incorpora las SCC de Serbia con Kyndryl actuando en nombre del Proveedor como Encargado del Tratamiento; y (ii) el Proveedor firmará acuerdos por escrito con cada Subencargado del Tratamiento aprobado, de conformidad con el Artículo 8 de las SCC de Serbia, y proporcionará a Kyndryl copias de dichos acuerdos, a petición.

(b) Si el Proveedor está establecido en un País Adecuado, el Proveedor incorpora las SCC de Serbia con Kyndryl actuando en nombre de cada Subencargado del Tratamiento ubicado en un País No Adecuado. Si el Proveedor no puede hacerlo para ningún Subencargado del Tratamiento, el Proveedor proporcionará a Kyndryl las SCC de Serbia firmadas por el Subencargado del Tratamiento para la posterior firma de Kyndryl antes de permitir que el Subencargado del Tratamiento trate los Datos Personales de Kyndryl.

(c) Las SCC de Serbia entre Kyndryl y el Proveedor servirán como las SCC de Serbia entre un Responsable del Tratamiento y un Encargado del Tratamiento o como un acuerdo por escrito consecutivo entre el 'Encargado del Tratamiento' y el 'Subencargado del Tratamiento', según lo requieran los hechos. En caso de conflicto entre las SCC de Serbia y estas Condiciones, prevalecerán las SCC de Serbia.

(d) La información necesaria para completar los Apéndices 1 a 8 de las SCC de Serbia para la finalidad de regular la transferencia de Datos Personales a un País No Adecuado se puede encontrar en estas Condiciones y en el Anexo al Documento Transaccional, o en el propio Documento Transaccional.

5.6 Acerca de los Anexos suizos:

(a) En el caso y en la medida en que una transferencia de datos personales de Kyndryl en virtud de la sección 5.1. esté sujeta a la Ley Federal Suiza sobre Protección de Datos («FADP»), las SCC de la UE acordadas en la Sección 5.2. de estos Términos regirán dicha transferencia con las siguientes enmiendas a fin de adoptar el estándar del RGPD para los datos personales suizos:

- Las referencias al Reglamento General de Protección de Datos («RGPD») se entenderán asimismo como referencias a las disposiciones homólogas de la FADP;
- el Comisionado Federal de Protección e Información de Datos será la autoridad de control competente en virtud de la Cláusula 13 y el Anexo I.C de las SCC de la UE;
- la legislación suiza será la legislación aplicable en caso de que la transferencia quede sujeta exclusivamente a la FADP; y
- El término «estado miembro» de la Cláusula 18 de las SCC de la UE se ampliará para incluir a Suiza con el fin de permitir que los interesados suizos ejerzan sus derechos en su lugar de residencia habitual.

(b) A fin de evitar confusiones, ninguno de los puntos anteriores tiene la intención de disminuir el nivel de protección de datos proporcionado por las SCC de la UE de ninguna manera, sino que simplemente pretenden ampliar dicho nivel de protección a los interesados suizos. En el caso y en la medida en que estas no sean las circunstancias, prevalecerán las SCC de la UE.

6. Asistencia y Registros

6.1 Teniendo en cuenta la naturaleza del Tratamiento, el Proveedor ayudará a Kyndryl mediante la adopción de medidas técnicas y organizativas adecuadas para 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 Tratamiento, la notificación y comunicación de una Brecha de Seguridad y la creación de evaluaciones de impacto de protección de datos, incluida la consulta previa con el regulador responsable, si es necesario, teniendo en cuenta la información disponible para el Proveedor.

6.2 El Proveedor mantendrá un registro actualizado del nombre y los detalles de contacto de cada Subencargado del Tratamiento, incluyendo el delegado de protección de datos y representante del Subencargado del Tratamiento. Previa solicitud, el Proveedor proporcionará este registro a Kyndryl bajo una programación que permita a Kyndryl responder puntualmente a cualquier demanda de un Cliente u otro tercero.

Artículo IV, Medidas Técnicas y Organizativas, Seguridad del Código

Este Artículo se aplica si el Proveedor tiene acceso al Código Fuente de Kyndryl. El Proveedor cumplirá los requisitos de este Artículo y al hacerlo protegerá el Código Fuente de Kyndryl frente a pérdida, destrucción, alteración, revelación accidental o no autorizada, acceso accidental o no autorizado y formas ilegales de Manejo. Los requisitos de este Artículo se extienden a todas las aplicaciones, plataformas e infraestructura de TI que el Proveedor opere o gestione para proporcionar Entregables y Servicios y en el Manejo de Tecnologías de Kyndryl, incluidos todos los entornos de desarrollo, prueba, alojamiento, soporte, operaciones y centros de datos.

1. Requisitos de Seguridad

Según su uso a continuación,

País Prohibido: cualquier país: (a) que el Gobierno de los Estados Unidos haya designado como adversario extranjero en virtud de la Orden Ejecutiva del 15 de mayo de 2019 sobre la Seguridad de la Cadena de Suministro de Tecnología y Servicios de Información y Comunicaciones, (b) indicado como conforme al Apartado 1654 de la Ley de Autorización de Defensa Nacional de EE. UU. de 2019, o (c) identificado como "País Prohibido" en el Documento Transaccional.

1.1. El Proveedor no distribuirá ni pondrá ningún Código Fuente de Kyndryl en depósito en beneficio de ningún tercero.

1.2. El Proveedor no permitirá que ningún Código Fuente de Kyndryl resida en servidores ubicados en un País Prohibido. El Proveedor no permitirá a nadie, incluido su Personal, ubicado en un País Prohibido o que visite un País Prohibido (durante el plazo de dicha visita), por ningún motivo, acceder o utilizar cualquier Código Fuente de Kyndryl, independientemente de dónde se encuentre el Código Fuente de Kyndryl a nivel global, y el Proveedor no permitirá que se realicen desarrollos, pruebas u otros trabajos en un País Prohibido que requiera dicho acceso o uso.

1.3. El Proveedor no pondrá ni distribuirá Código Fuente de Kyndryl en ninguna jurisdicción donde la ley o la interpretación de la ley exijan la revelación del Código Fuente a terceros. Si se produce un cambio de ley o de interpretación de la ley en una jurisdicción donde se encuentra el Código Fuente de Kyndryl, que pueda obligar al Proveedor a revelar el Código Fuente a un tercero, el Proveedor destruirá o eliminará inmediatamente el Código Fuente de Kyndryl de dicha jurisdicción, y no pondrá ningún Código Fuente de Kyndryl adicional en dicha jurisdicción si la ley o la interpretación de la ley sigue vigente.

1.4. El Proveedor no llevará a cabo, directa o indirectamente, ninguna acción, incluida la firma de un acuerdo, que pueda causar que el Proveedor, Kyndryl o cualquier tercero incurra en una obligación de revelación bajo los Apartados 1654 o 1655 de la Ley de Autorización de Defensa Nacional de EE. UU. de 2019. Para mayor claridad, salvo que se permita expresamente en el Documento Transaccional o el acuerdo base asociado entre las partes, el Proveedor no puede revelar el Código Fuente de Kyndryl a ningún tercero, bajo ninguna circunstancia, sin el consentimiento previo por escrito de Kyndryl.

1.5. Si Kyndryl notifica al Proveedor, o un tercero notifica a cualquiera de las partes, que: (a) el Proveedor ha permitido que el Código Fuente de Kyndryl se lleve a un País Prohibido o a cualquier jurisdicción sujeta al Apartado 1.3 anterior, (b) el Proveedor ha publicado, accedido o utilizado el Código Fuente de Kyndryl de una manera no permitida por el Documento Transaccional o la base asociada u otro acuerdo entre las partes o (c) el Proveedor ha infringido el Apartado 1.4 anterior, en consecuencia y sin limitar los derechos de Kyndryl para abordar dicho incumplimiento de forma legal o justa o según el Documento Transaccional o la base asociada u otro acuerdo entre las partes: (i) si dicha notificación se realiza al Proveedor, el Proveedor compartirá de inmediato la notificación con Kyndryl; y (ii) el Proveedor, bajo directrices razonables de Kyndryl, investigará y corregirá el asunto bajo la programación que Kyndryl determine razonablemente (tras consultarlo con el Proveedor).

1.6. Si Kyndryl considera razonablemente que pueden ser necesarios cambios en las políticas, procedimientos, controles o prácticas del Proveedor con respecto al acceso al Código Fuente para abordar la ciberseguridad, el robo de propiedad intelectual o riesgos similares o relacionados (incluido el riesgo de que la no aplicación de estos cambios suponga que Kyndryl no pueda vender a ciertos

Clientes o en determinados mercados o no pueda satisfacer los requisitos de seguridad del cliente o de la cadena de suministro), Kyndryl puede ponerse en contacto con el Proveedor para debatir las acciones necesarias para abordar los riesgos, incluidos los cambios en dichas políticas, procedimientos, controles o prácticas. A petición de Kyndryl, el Proveedor cooperará con Kyndryl para evaluar si los cambios son necesarios y para implementar los cambios apropiados y mutuamente acordados.

Artículo V, Desarrollo Seguro

Este Artículo se aplica si el Proveedor proporcionará su Código Fuente o Software Local o el de un tercero a Kyndryl, o si se proporcionará cualquiera de los Entregables o Servicios del Proveedor a un Cliente de Kyndryl como parte de un producto o servicio de Kyndryl.

1. Preparación de la Seguridad

El Proveedor cooperará con procesos internos de Kyndryl que evalúan la preparación de la seguridad de los productos y servicios de Kyndryl que dependen de cualquiera de los Entregables del Proveedor, incluyendo la respuesta oportuna a las solicitudes de información, ya sea a través de documentos, otros registros, entrevistas del Personal del Proveedor relevante o similares.

2. Desarrollo seguro

2.1 Esta Sección 2 solo se aplica cuando el Proveedor proporciona Software Local a Kyndryl.

2.2 El Proveedor ha implementado y mantendrá durante la vigencia del Documento Transaccional, de acuerdo con las Prácticas Recomendadas del Sector, la red, la plataforma, el sistema, la aplicación, el dispositivo, la infraestructura física, la respuesta a incidencias y las políticas, los procedimientos y los controles de seguridad centrados en el Personal que son necesarios para proteger : (a) los sistemas y entornos de desarrollo, compilación, pruebas y operaciones que el Proveedor o cualquier tercero contratado por el Proveedor opera, administra, utiliza o en los que confía de otro modo para o con respecto a los Entregables y (b) todo el código fuente de Entregables contra la pérdida, formas ilegales de manejo y el acceso, la divulgación o la modificación sin autorización.

3. Certificación ISO 20243

3.1 Esta Sección 3 solo se aplica si alguno de los Entregables o Servicios del Proveedor se proporcionará a un Cliente de Kyndryl como parte de un producto o servicio de Kyndryl.

3.2 El Proveedor obtendrá una certificación de conformidad con ISO 20243, Tecnología de la Información, Proveedor de Tecnología de Confianza Abierta, Estándar TM (O-TTPS), Mitigación de productos malintencionados y falsificados (ya sea una certificación autoevaluada o una certificación basada en la evaluación de un auditor independiente de buena reputación). Como alternativa, si el Proveedor lo solicita por escrito e Kyndryl lo aprueba por escrito, el Proveedor obtendrá una certificación de conformidad con una norma del sector sustancialmente equivalente que aborde prácticas de cadena de suministro y desarrollo seguro (ya sea una certificación autoevaluada o una certificación basada en la evaluación de un auditor independiente de buena reputación, si Kyndryl lo aprueba).

3.3 El Proveedor obtendrá la certificación de conformidad con la norma ISO 20243 o una norma del sector sustancialmente equivalente (si Kyndryl lo aprueba por escrito) 180 días después de la fecha efectiva del Documento Transaccional y posteriormente renovará la certificación cada 12 meses a partir de este momento (con cada renovación conforme a la versión más actual de la norma aplicable, es decir, ISO 20243 o, si Kyndryl lo ha aprobado por escrito, una norma del sector sustancialmente equivalente que aborde prácticas de cadena de suministro o desarrollo seguro).

3.4 El Proveedor, a petición, proporcionará a Kyndryl una copia de las certificaciones que el Proveedor está obligado a obtener, según los Apartados 2.1 y 2.2 anteriores.

4. Vulnerabilidades de Seguridad

Según su uso a continuación,

Corrección de error: arreglos de defectos y revisiones que corrigen errores o deficiencias, incluyendo las Vulnerabilidades de Seguridad, en los Entregables.

Mitigación: cualquier medio conocido de reducir o evitar los riesgos de una Vulnerabilidad de Seguridad.

Vulnerabilidad de Seguridad: un estado en el diseño, codificación, desarrollo, implementación, prueba, operación, soporte, mantenimiento o gestión de un Entregable que permite un ataque que puede dar como resultado la explotación o el acceso no autorizado, incluyendo: (a) acceso, control o interrupción de la operación de un sistema, (b) acceso, supresión, modificación o extracción de datos, o (c) cambios de identidad, autorizaciones o permisos de usuarios o administradores. Una Vulnerabilidad de Seguridad puede existir independientemente de si se le ha asignado un ID de Vulnerabilidades y Exposiciones Comunes (CVE) o cualquier otra puntuación o clasificación oficial.

4.1 El Proveedor declara y garantiza que: (a) utilizará Prácticas Recomendadas del Sector para identificar las Vulnerabilidades de Seguridad, incluyendo de forma continua la exploración de seguridad de aplicaciones de código abierto estático y dinámico, la exploración de seguridad de código abierto y la exploración de vulnerabilidades del sistema, y (b) cumplirá los requisitos de estas Condiciones para ayudar a evitar, detectar y corregir las Vulnerabilidades de Seguridad en los Entregables y en todas las aplicaciones, plataformas e infraestructuras de TI con las que el Proveedor cree y proporcione Servicios y Entregables.

4.2 Si el Proveedor tiene conocimiento de una Vulnerabilidad de Seguridad en un Entregable o en alguna de estas aplicaciones, plataformas e infraestructuras de TI, el Proveedor deberá proporcionar a Kyndryl una Mitigación y Corrección de Errores para todas las versiones y lanzamientos de los Entregables de acuerdo con los Niveles de Gravedad y periodos de tiempo que se definen en las tablas siguientes:

Nivel de Gravedad*
Vulnerabilidad de Seguridad de Emergencia: Vulnerabilidad de Seguridad que constituye una amenaza grave y potencialmente global. Kyndryl designa las Vulnerabilidades de Seguridad de Emergencia bajo su criterio exclusivo, independientemente de su Puntuación Base de CVSS.
Crítica: una Vulnerabilidad de Seguridad con una Puntuación Base de CVSS de 9 a 10,0
Alta: una Vulnerabilidad de Seguridad con una Puntuación Base de CVSS de 7,0 a 8,9
Media: una Vulnerabilidad de Seguridad con una Puntuación Base de CVSS de 4,0 a 6,9
Baja: una Vulnerabilidad de Seguridad con una Puntuación Base de CVSS de 0,0 a 3,9

Plazos				
Emergencia	***Crítico***	***Alta***	***Media***	***Baja***
4 días o menos, según determine la Oficina de Seguridad de la Información Principal de Kyndryl	30 días	30 días	90 días	Según la Prácticas Recomendadas del Sector

* En cualquier caso en que una Vulnerabilidad de Seguridad no tenga una Puntuación Base de CVSS asignada con prontitud, el Proveedor aplicará un Nivel de Gravedad apropiado a la naturaleza y las circunstancias de la vulnerabilidad.

4.3 Para una Vulnerabilidad de Seguridad que se haya revelado públicamente y para la que el Proveedor no haya proporcionado todavía a Kyndryl una Mitigación y Corrección de Errores, el Proveedor deberá implementar controles de seguridad adicionales viables que puedan mitigar los riesgos de la vulnerabilidad.

4.4 Si Kyndryl no está satisfecho con la respuesta del Proveedor a cualquier Vulnerabilidad de Seguridad en un Entregable o en cualquier aplicación, plataforma o infraestructura mencionada anteriormente, sin perjuicio de cualquier otro derecho de Kyndryl, el Proveedor facilitará de inmediato que Kyndryl pueda debatir sus inquietudes directamente con un vicepresidente o un ejecutivo equivalente del Proveedor que sea responsable de proporcionar la Corrección del Error.

4.5 Ejemplos de Vulnerabilidades de Seguridad incluyen código de terceros o código fuente abierto de fin de servicio (EOS), dado que estos tipos de código ya no reciben fixes de seguridad.

Artículo VI, Acceso a Sistemas Corporativos

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

1. Condiciones generales

1.1 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.

1.2 Kyndryl identificará los medios por los cuales los empleados del Proveedor pueden acceder a los Sistemas Corporativos, incluyendo si los empleados tendrán acceso a los Sistemas Corporativos a través de Kyndryl o de los Dispositivos proporcionados por el Proveedor.

1.3 Los empleados del Proveedor solo pueden acceder a los Sistemas Corporativos, y solo pueden usar los Dispositivos que Kyndryl autorice para el acceso, para prestar Servicios. Los empleados del Proveedor no pueden usar los Dispositivos que Kyndryl autorice 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.

1.4 Para mayor claridad, los empleados del Proveedor no pueden usar los Dispositivos que Kyndryl autoriza para acceder a los Sistemas Corporativos por ningún motivo personal (por ejemplo, los empleados del Proveedor no pueden almacenar archivos personales como música, vídeos, imágenes u otros elementos similares en dichos Dispositivos y no pueden usar Internet desde dichos dispositivos por razones personales).

1.5 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 un lápiz USB, un disco duro externo u otros elementos similares).

1.6 A petición, el Proveedor confirmará, por nombre de 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.

1.7 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 ya no: (a) sea empleado por el Proveedor o (b) trabaje en actividades que requieran dicho acceso. El Proveedor trabajará con Kyndryl para garantizar que se revoque de inmediato el acceso de dichos ex-empleados o empleados actuales.

1.8 El Proveedor notificará inmediatamente a Kyndryl cualquier incidente de seguridad real o sospechado (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) a Kyndryl y cooperará con Kyndryl en la investigación de dichos incidentes.

1.9 El Proveedor no puede permitir que ningún agente, contratista independiente o empleado subcontratista acceda a ningún sistema corporativo, sin el consentimiento previo por escrito de Kyndryl; Si Kyndryl proporciona ese consentimiento, el Proveedor implicará 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 a al acceso al Sistema Corporativo.

2. Software del Dispositivo

2.1 El Proveedor ordenará a sus empleados que instalen oportunamente todo el software del Dispositivo que Kyndryl requiera para facilitar el acceso a los Sistemas Corporativos de manera segura. Ni el Proveedor ni sus empleados interferirán en las operaciones del software o las características de seguridad que el software permite.

2.2 El Proveedor y sus empleados cumplirán las reglas de configuración del Dispositivo que Kyndryl establezca y de otro modo trabajarán con Kyndryl para ayudar a garantizar que el software funcione

como Kyndryl pretende. Por ejemplo, el Proveedor no anulará el bloqueo de páginas web de software o las características de parches automáticos.

2.3 Los empleados del Proveedor no pueden compartir los Dispositivos que utilizan para acceder a los sistemas corporativos, o los nombres de usuario, contraseñas o similares de los Dispositivos con cualquier otra persona.

2.4 Si Kyndryl autoriza a los empleados 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 del sistema operativo o un nuevo sistema operativo, en un plazo razonable, después de que Kyndryl así lo indique.

3. Supervisión y Cooperación

3.1 Kyndryl dispone de los derechos no calificados para supervisar 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, (a) realizar una prueba de seguridad en cualquier Dispositivo, (b) 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 o transmitidos a través de cualquier Sistema Corporativo, y (c) adquirir una imagen forense completa de cualquier Dispositivo. 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, instalar software de supervisión o de otro tipo en cualquier Dispositivo, compartir detalles de conexión a nivel del sistema, participar en medidas de respuesta a incidentes en cualquier Dispositivo y proporcionar acceso físico a cualquier Dispositivo para que Kyndryl obtenga una imagen forense completa o de otro tipo, y solicitudes similares y relacionadas).

3.2 Kyndryl puede revocar el acceso a los Sistemas Corporativos en cualquier momento, para cualquier empleado del Proveedor o para todos los empleados del Proveedor, sin previo aviso al Proveedor, a cualquier empleado del Proveedor o a otros, si Kyndryl cree que es necesario para proteger a Kyndryl.

3.3 Los derechos de Kyndryl no quedan bloqueados, reducidos o restringidos de ninguna manera por ninguna cláusula del Documento Transaccional, el acuerdo base asociado entre las partes o cualquier otro acuerdo entre las partes, incluida cualquier cláusula que pueda requerir datos, materiales u otra información de cualquier tipo que resida solo en una ubicación o en ubicaciones seleccionadas o que pueda requerir que solo personas de una ubicación o de ubicaciones seleccionadas accedan a dichos datos, materiales u otra información.

4. Dispositivos de Kyndryl

4.1 Kyndryl retendrá la titularidad de todos los Dispositivos de Kyndryl, y el Proveedor asumirá el riesgo de pérdida de los Dispositivos, incluyendo 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.

4.2 El Proveedor devolverá todos los Dispositivos de Kyndryl dentro del plazo de 5 días laborables tras la finalización de la necesidad de que dichos Dispositivos proporcionen 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 las Prácticas Recomendadas del Sector 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 costes, en la ubicación que

Kyndryl identifique. El incumplimiento por parte del Proveedor de cualquier obligación establecida en este Apartado 4.2 constituye una infracción sustancial del Documento Transaccional 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.

4.3 Kyndryl proporcionará soporte para Dispositivos 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.

4.4 Para los programas de software que Kyndryl posea o de los cuales tenga derecho para conceder licencia, Kyndryl otorga al Proveedor un derecho temporal para usar, almacenar y hacer copias suficientes para dar soporte a su uso autorizado de Dispositivos 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.

5. Actualizaciones

5.1 Sin perjuicio de lo establecido en contra en el Documento Transaccional o el acuerdo base asociado entre las partes, previa notificación por escrito al Proveedor y sin necesidad de obtener el consentimiento del Proveedor, Kyndryl puede actualizar, complementar o de otro modo enmendar este Artículo para abordar cualquier requisito bajo la legislación aplicable o una obligación del Cliente, para reflejar cualquier desarrollo en prácticas recomendadas de seguridad, o de otra manera como Kyndryl considere necesario para proteger los Sistemas Corporativos o a Kyndryl.

Artículo VII, Aumento de Personal

Este Artículo se aplica cuando los empleados de Proveedor dedicarán todo su tiempo laborable a prestar Servicios para Kyndryl, realizarán todos esos Servicios en las instalaciones de Kyndryl, en las instalaciones del Cliente o desde sus casas, y solo proporcionarán Servicios usando los Dispositivos de Kyndryl para acceder a los Sistemas Corporativos.

1. Acceso a Sistemas Corporativos; Entornos de Kyndryl

1.1 El Proveedor solo puede realizar Servicios accediendo a Sistemas Corporativos utilizando los Dispositivos que Kyndryl proporciona.

1.2 El Proveedor cumplirá con las condiciones establecidas en el Artículo VI (Acceso a Sistemas Corporativos), para todo acceso a los Sistemas Corporativos.

1.3 Los Dispositivos proporcionados por Kyndryl son los únicos Dispositivos que el Proveedor y sus empleados pueden usar para prestar Servicios y solo pueden utilizarlos el Proveedor y sus empleados para prestar Servicios. Para mayor claridad, en ningún caso el Proveedor o sus empleados pueden usar ningún otro Dispositivo para prestar Servicios o utilizar Dispositivos de Kyndryl para cualquier otro cliente del Proveedor o para cualquier otro propósito que no sea prestar Servicios a Kyndryl.

1.4 Los empleados del Proveedor que usan Dispositivos de Kyndryl pueden compartir Materiales de Kyndryl entre ellos y almacenar dichos materiales en los Dispositivos de Kyndryl, pero solo en la medida limitada en que dicho intercambio y almacenamiento sean necesarios para prestar con éxito los Servicios.

1.5 Excepto en lo relativo a dicho almacenamiento dentro de los Dispositivos de Kyndryl, en ningún caso el Proveedor o sus empleados pueden eliminar Materiales de Kyndryl de los repositorios, entornos, herramientas o infraestructura de Kyndryl donde Kyndryl los conserve.

1.6 Para mayor claridad, ni el Proveedor ni sus empleados están autorizados a transferir Materiales de Kyndryl a los repositorios, entornos, herramientas o infraestructura del Proveedor, ni a ningún otro sistema, plataforma, redes o infraestructura similar del Proveedor, sin el consentimiento previo por escrito de Kyndryl.

1.7 El Artículo VIII (Medidas Técnicas y Organizativas, Seguridad General) no se aplica a los Servicios del Proveedor en los casos en que los empleados del Proveedor dediquen todo su tiempo laborable a prestar Servicios para Kyndryl, presten todos esos Servicios en las instalaciones de Kyndryl, las instalaciones del Cliente o desde sus hogares, y solo proporcionen Servicios que utilizan Dispositivos de Kyndryl para acceder a los Sistemas Corporativos. En cualquier otro caso, el Artículo VIII se aplica a los Servicios del Proveedor.

Artículo VIII, Medidas Técnicas y Organizativas, Seguridad General

Este artículo se aplica si el Proveedor proporciona algún Servicio o Entregables a Kyndryl, a menos que el Proveedor solo tenga acceso a la BCI de Kyndryl para proporcionar esos Servicios y Entregables (por ejemplo, el Proveedor no tratará otros Datos de Kyndryl ni tendrá acceso a ningún otro tipo de Materiales de Kyndryl ni a ningún sistema corporativo) o el Proveedor proporciona todos sus Servicios y Entregables bajo un modelo de ampliación de personal de conformidad con el Artículo VII, incluido su Apartado 1.7.

El Proveedor cumplirá los requisitos de este Artículo y al hacerlo protegerá: (a) los Materiales de Kyndryl contra pérdida, destrucción, alteración, revelación accidental o no autorizada, y accidental o acceso no autorizado, (b) los Datos de Kyndryl frente a formas ilegales de Tratamiento y (c) la Tecnología de Kyndryl frente a formas ilegales de Manejo. Los requisitos de este Artículo se extienden a todas las aplicaciones, plataformas e infraestructura de TI que el Proveedor opere o gestione para proporcionar Entregables y Servicios y en el Manejo de Tecnologías de Kyndryl, incluidos todos los entornos de desarrollo, prueba, alojamiento, soporte, operaciones y centros de datos.

1. Políticas de Seguridad

1.1. El Proveedor mantendrá y seguirá las políticas y prácticas relativas a la seguridad de TI que formen parte del negocio del Proveedor, sean obligatorias para todos los empleados del Proveedor y sean coherentes con las Prácticas Recomendadas del Sector.

1.2. El Proveedor revisará sus políticas y prácticas de seguridad de TI como mínimo una vez al año y realizará modificaciones de las mismas según sea necesario para proteger los Materiales de Kyndryl.

1.3. El Proveedor actualizará y seguirá sus requisitos obligatorios de verificación de empleabilidad en las nuevas contrataciones y ampliará tales requisitos a todo el Personal del Proveedor y a las filiales bajo propiedad integral del Proveedor. Dichos requisitos incluirán comprobaciones de antecedentes criminales, 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.

1.4. El Proveedor proporcionará una formación sobre seguridad y privacidad a sus empleados anualmente, y requerirá que todos los empleados certifiquen cada año que van a cumplir con las políticas éticas del Proveedor respecto a la conducta empresarial, la confidencialidad y la seguridad, como se establece en el código de conducta del Proveedor o en documentos similares. El Proveedor proporcionará una formación complementaria sobre procesos y políticas al personal con acceso administrativo a los componentes de los Servicios, Entregables o Materiales de Kyndryl, que será específica para su función y el soporte de los Servicios, Entregables y Materiales de Kyndryl, y necesaria para mantener la conformidad y las certificaciones necesarias.

1.5. El Proveedor diseñará medidas de seguridad y privacidad para proteger y mantener la disponibilidad de los Materiales de Kyndryl, incluido mediante su implementación, mantenimiento y cumplimiento de las políticas y los procedimientos que requieren privacidad y seguridad por diseño, ingeniería segura y operaciones seguras, para todos los Servicios y Entregables y para todo el Manejo de Tecnologías de Kyndryl.

2. Incidentes de Seguridad

2.1. El Proveedor mantendrá y seguirá las políticas de respuesta a incidentes conforme a las Prácticas Recomendadas del Sector para la administración de incidentes de seguridad informática.

2.2. El Proveedor investigará cualquier acceso no autorizado o uso no autorizado de los Materiales de Kyndryl y definirá y ejecutará un plan de respuesta adecuado.

2.3. El Proveedor avisará a Kyndryl inmediatamente (y en ningún caso más tarde de 48 horas) tras conocer cualquier brecha de seguridad. El proveedor proporcionará dicha notificación a cyber.incidents@kyndryl.com. El Proveedor suministrará a Kyndryl la información razonablemente solicitada acerca de la infracción y del estado de las actividades de corrección y restauración llevadas a cabo por cualquier Proveedor. A modo de ejemplo, la información solicitada razonablemente puede incluir registros que demuestren acceso privilegiado, administrativo y de otro tipo a Dispositivos, sistemas o aplicaciones, imágenes forenses de Dispositivos, sistemas o aplicaciones y otros elementos similares, en la medida que sean relevantes con la infracción o las actividades de reparación y restauración del Proveedor.

2.4. El Proveedor proporcionará asistencia razonable a Kyndryl en el cumplimiento de las obligaciones legales (incluida la obligación de notificar a los reguladores o los Interesados) de Kyndryl, las filiales de Kyndryl y los Clientes (y sus respectivos clientes y filiales) en relación con la Brecha de Seguridad.

2.5. El Proveedor no informará ni notificará a ningún tercero de que una Infracción de Seguridad está relacionada directa o indirectamente con Kyndryl o los Materiales de Kyndryl a menos que Kyndryl apruebe hacerlo por escrito o cuando así lo requiera la ley. El Proveedor debe notificar a Kyndryl por escrito antes de la distribución de cualquier notificación legalmente requerida a cualquier tercero, donde la notificación revelaría directa o indirectamente la identidad de Kyndryl.

2.6. En caso de producirse una Brecha de Seguridad que surja del incumplimiento por parte del Proveedor de cualquier obligación bajo estas Condiciones:

(a) el Proveedor será responsable de los costes incurridos por el Proveedor, así como de los costes reales en que incurra Kyndryl, al notificar la Brecha de Seguridad a los reguladores correspondientes, otros organismos gubernamentales y los organismos autorreguladores de la industria pertinente, los medios (si lo requiere la legislación aplicable), Interesados, Clientes, etc.,

(b) si Kyndryl lo solicita, el Proveedor establecerá y mantendrá a su cargo un centro de atención telefónica para responder a las preguntas de los Interesados sobre la Brecha de Seguridad y sus consecuencias, durante 1 año después de la fecha en que dichos Interesados hayan sido notificados acerca de la Brecha de Seguridad, o según lo requiera cualquier legislación de protección de datos aplicable, lo que brinde mayor protección. Kyndryl y el Proveedor trabajarán juntos para crear los scripts y otros materiales que utilizará el personal del centro de atención telefónica para responder a las consultas. Alternativamente, mediante notificación escrita al Proveedor, Kyndryl puede establecer y mantener su propio centro de atención telefónica, en lugar de que lo establezca el Proveedor, y el Proveedor reembolsará a Kyndryl los costes reales en que incurra Kyndryl para establecer y mantener dicho centro de atención telefónica, y

(c) el Proveedor reembolsará a Kyndryl los costes reales en que incurra Kyndryl al prestar Servicios de supervisión y restauración de crédito durante 1 año después de la fecha en que las personas afectadas por la brecha que elijan registrarse para recibir estos servicios hayan sido notificadas acerca de las Brechas de Seguridad, o según lo requiera cualquier legislación de protección de datos aplicable, lo que brinde mayor protección.

3. Seguridad Física y Control de Entrada (como se usa a continuación, "Instalación" significa una ubicación física donde el Proveedor aloja, trata o accede de otro modo a Materiales de Kyndryl).

3.1. El Proveedor efectuará los controles de entrada física adecuados, como barreras, puntos de entrada controlados con tarjeta, cámaras de vigilancia y recepcionistas, para impedir la entrada no autorizada a las Instalaciones.

3.2. El Proveedor requerirá una aprobación autorizada para acceder a las Instalaciones y áreas controladas dentro de las Instalaciones, incluido cualquier acceso temporal, y limitará el acceso según la función profesional y la necesidad empresarial. Si el Proveedor otorga acceso temporal, su empleado autorizado escoltará al visitante mientras esté en las Instalaciones y las áreas controladas.

3.3. El Proveedor implementará controles de acceso físico, incluidos los controles de acceso de varios factores que serán coherentes con las Prácticas Recomendadas del Sector, para restringir adecuadamente la entrada a las áreas controladas dentro de las Instalaciones, registrará todos los intentos de entrada y guardará dichos registros durante un año como mínimo.

3.4. El Proveedor revocará el acceso a las Instalaciones y áreas controladas dentro de las Instalaciones (a) tras la separación de un empleado autorizado del Proveedor o (b) cuando el empleado autorizado del Proveedor ya no tenga una necesidad empresarial de acceso. El Proveedor llevará a cabo los procedimientos formales de terminación de la relación laboral que incluyen la eliminación de las listas de control de acceso y la devolución de los identificadores de acceso físicos.

3.5. El Proveedor tomará precauciones para proteger toda la infraestructura física utilizada para dar soporte a los Servicios y Entregables y el Manejo de Tecnologías de Kyndryl frente a amenazas medioambientales, tanto naturales como artificiales, como temperatura ambiental excesiva, incendios, inundaciones, humedad, robo y vandalismo.

4. Acceso, Intervención, Transferencia y Control de Segregación de Funciones

4.1. El Proveedor mantendrá la arquitectura de seguridad documentada de las redes que gestiona en su operativa de los Servicios, su provisión de Entregables y su Manejo de Tecnologías de Kyndryl. El Proveedor revisará de forma independiente la arquitectura de red y utilizará medidas para evitar las conexiones de red no autorizadas a sistemas, aplicaciones y dispositivos de red, para el cumplimiento de las normas de segmentación segura, aislamiento y defensa en profundidad. El Proveedor no puede utilizar tecnología inalámbrica en sus alojamientos y operaciones de Servicios Alojados; de lo contrario, el Proveedor puede utilizar tecnología de red inalámbrica en su prestación de los Servicios y los Entregables y en su Manejo de Tecnologías de Kyndryl, pero el Proveedor deberá cifrar y requerir una autenticación segura para dichas redes inalámbricas.

4.2. El Proveedor actualizará las medidas diseñadas para separar lógicamente e impedir la exposición o el acceso a Materiales de Kyndryl de personas no autorizadas. Asimismo, 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.

4.3. El Proveedor cifrará los Materiales de Kyndryl en tránsito y en reposo (a menos que el Proveedor demuestre de forma razonable a Kyndryl que el cifrado de los Materiales de Kyndryl en reposo es técnicamente inviable). El Proveedor también cifrará todos los soportes físicos, si existen, como los que contienen archivos de copia de seguridad. El Proveedor actualizará los procedimientos documentados para la generación, emisión, distribución, almacenamiento, rotación, revocación, recuperación, copia de seguridad, destrucción, acceso y uso de claves seguras asociados con el cifrado de datos. El Proveedor se asegurará de que los métodos criptográficos específicos utilizados para dicho cifrado se alineen con las Prácticas Recomendadas del Sector como, por ejemplo, NIST SP 800-131a.

4.4. Si el Proveedor requiere acceso a Materiales de Kyndryl, el Proveedor restringirá y limitará dicho acceso al nivel mínimo necesario para la prestación y el soporte de los Servicios y los Entregables. El Proveedor requerirá que dicho acceso, incluido el acceso administrativo a los componentes subyacentes (por ejemplo, acceso con privilegios), será individual, se basará en cargos y estará sujeto a aprobación y validación regular por parte del Personal del Proveedor autorizado conforme a los principios de separación de funciones. El Proveedor mantendrá medidas adecuadas para identificar y eliminar cuentas redundantes e iniciativas. El Proveedor también revocará las cuentas con acceso privilegiado dentro del plazo de veinticuatro (24) horas posterior a la separación del titular de la cuenta o a la solicitud por parte Kyndryl o cualquier empleado del Proveedor autorizado, como el director del titular de la cuenta.

4.5. De conformidad con las Prácticas Recomendadas del Sector, el Proveedor mantendrá medidas técnicas que impongan tiempo de espera en sesiones inactivas, bloqueo de cuentas tras diversos intentos fallidos de inicio de sesión, autenticación con contraseña o frase de contraseña fuerte, así como medidas que requieran la transferencia y el almacenamiento seguros de estas contraseñas y frases de contraseñas. Asimismo, el Proveedor utilizará la autenticación de varios factores para todo acceso con privilegios no basado en contraseña a los Materiales de Kyndryl.

4.6. El Proveedor supervisará el uso del acceso con privilegios y mantendrá la información de seguridad y las medidas de gestión de eventos diseñadas para (a) identificar la actividad y el acceso no autorizados; (b) facilitar una respuesta adecuada y oportuna a la actividad y el acceso no autorizados; y (c) habilitar las auditorías del Proveedor, Kyndryl (de acuerdo con sus derechos de verificación de estas Condiciones y derechos de auditoría de este Documento Transaccional o base asociada u otro acuerdo relacionado entre las partes) y otros de acuerdo con la política documentada del Proveedor.

4.7. El Proveedor mantendrá unos registros en los que incorporará, de conformidad con las Prácticas Recomendadas del Sector, todos los accesos o actividades administrativas, de usuarios o de otro tipo para o con respecto a los sistemas utilizados para prestar Servicios o Entregables y en el Manejo de Tecnologías de Kyndryl (y proporcionará esos registros a Kyndryl, a petición). El Proveedor mantendrá medidas diseñadas para la protección en caso de acceso no autorizado, modificación y destrucción accidental o deliberada de estos registros.

4.8. El Proveedor mantendrá medidas informáticas de protección para los sistemas que posee o gestiona, incluidos los sistemas de usuario final, y que utilice para prestar Servicios o Entregables o en el Manejo

de Tecnologías de Kyndryl, y estas medidas de protección incluirán lo siguiente: los cortafuegos de puntos finales, el cifrado de disco completo, las tecnologías de detección y respuesta de punto final basadas en firmas y no basadas en firmas para detectar malware y amenazas persistentes avanzadas, los bloqueos de pantalla basados en tiempo y las soluciones de gestión de puntos finales que impongan tanto la configuración de seguridad como los requisitos de parches. Asimismo, el Proveedor implementará controles técnicos y operativos que garanticen que solo los sistemas de usuario final conocidos y de confianza puedan utilizar las redes del Proveedor.

4.9. De conformidad con las Prácticas Recomendadas del Sector, el Proveedor mantendrá protecciones para los entornos de centro de datos donde existan o se traten Materiales de Kyndryl. Dichas protecciones incluyen detección y prevención de intrusiones, y mitigación y contramedidas de ataques de denegación de servicio.

5. Integridad de Sistemas y Servicio y Control de Disponibilidad

5.1. El Proveedor (a) realizará evaluaciones de riesgos de seguridad y evaluación de vulnerabilidades al menos una vez al año, (b) llevará a cabo pruebas de intrusión y evaluaciones de vulnerabilidades, incluyendo el escaneo de seguridad automatizado de aplicaciones y sistemas y los pirateos éticos manuales, antes del lanzamiento en producción y anualmente a partir del mismo, (c) presentará un tercero independiente y cualificado para la realización de pruebas de penetración coherentes con las Prácticas Recomendadas del Sector al menos una vez al año, y estas pruebas incluirán pruebas manuales y automatizadas, (d) efectuará tareas de gestión automatizada y verificación rutinaria del cumplimiento de los requisitos de la configuración de seguridad de cada componente de los Servicios y los Entregables con respecto a su Manejo de Tecnologías de Kyndryl; y (e) corregirá las vulnerabilidades identificadas o el incumplimiento de los requisitos de la configuración de seguridad según el riesgo asociado, la posibilidad de explotación y el impacto. El Proveedor llevará a cabo los pasos razonables para evitar la interrupción de los Servicios durante la realización de las pruebas, evaluaciones y escaneos, así como durante la ejecución de las actividades de corrección. Si Kyndryl lo solicita, el Proveedor proporcionará a Kyndryl un resumen escrito de las actividades de pruebas de intrusión más recientes del Proveedor, cuyo informe incluirá como mínimo el nombre de las ofertas cubiertas por la prueba, el número de sistemas o aplicaciones en ámbito para las pruebas, las fechas de las pruebas, las metodologías utilizas en ellas y un resumen de alto nivel de los resultados.

5.2. El Proveedor mantendrá sus políticas y procedimientos diseñados para gestionar los riesgos asociados con la aplicación de cambios a los Servicios o Entregables o al Manejo de Tecnologías de Kyndryl. Antes de implementar dicho cambio, incluidos los sistemas, las redes y los componentes subyacentes afectados, el Proveedor documentará en una solicitud de cambio registrada: (a) una descripción y el motivo del cambio, (b) detalles y programación de implementación, (c) una declaración de riesgo que aborde el impacto en los Servicios y Entregables, clientes de los Servicios o Materiales de Kyndryl, (d) el resultado esperado, (e) plan de reversión y (f) aprobación por parte de los empleados autorizados del Proveedor.

5.3. El Proveedor mantendrá un inventario de todos los activos de TI que utiliza para operar los Servicios, proporcionar Entregables y el Manejo de Tecnologías de Kyndryl. El Proveedor supervisará y gestionará de forma continuada el estado (incluida la capacidad) y la disponibilidad de dichos activos de TI, Servicios, Entregables y Tecnologías de Kyndryl, incluidos los componentes subyacentes de dichos activos, Servicios, Entregables y Tecnologías de Kyndryl.

5.4. El Proveedor construirá todos los sistemas que utiliza en el desarrollo o la operación de Servicios y Entregables y en el Manejo de Tecnologías de Kyndryl a partir de líneas base de seguridad o imágenes de seguridad del sistema predefinidas, que cumplirán las Prácticas Recomendadas del Sector, como los indicadores del Centro de Seguridad de Internet (CIS).

5.5. Sin limitación de las obligaciones del Proveedor o los derechos de Kyndryl bajo el Documento Transaccional o el acuerdo base asociado entre las partes con respecto a la continuidad del negocio, el Proveedor evaluará por separado cada Servicio y Entregable y cada sistema de TI utilizado en el Manejo de Tecnologías de Kyndryl en relación con los requisitos de continuidad empresarial y TI y la recuperación tras desastre ("disaster recovery") de conformidad con las directrices documentadas de gestión de riesgos. El Proveedor garantizará que cada Servicio, Entregable y sistema de TI tenga, en la medida en que se especifique en la evaluación de riesgos, planes de recuperación tras desastre y

continuidad del negocio validados anualmente, mantenidos, documentados y definidos por separado conforme a las Prácticas Recomendadas del Sector. El Proveedor garantizará que dichos planes estén diseñados para ofrecer los tiempos de recuperación que se establecen en el Apartado 5.6, a continuación.

5.6. Los objetivos de punto de recuperación ("**RPO**") y los objetivos de tiempo de recuperación ("**RTO**") específicos en relación con un Servicio Alojado son: 24 horas de RPO y 24 horas de RTO; no obstante, el Proveedor cumplirá con cualquier RPO o RTO de menor duración para el que Kyndryl se haya comprometido con un Cliente, inmediatamente después de que Kyndryl notifique al Proveedor por escrito dicho RPO o RTO de menor duración (un correo electrónico se considera por escrito). En lo que respecta a los demás Servicios proporcionados por el Proveedor a Kyndryl, el Proveedor garantizará que sus planes de continuidad empresarial y recuperación tras desastre estén diseñados para proporcionar un RPO y RTO que permitan al Proveedor cumplir todas sus obligaciones con Kyndryl bajo este Documento Transaccional y el acuerdo base asociado entre las partes, y estas Condiciones, incluyendo sus obligaciones de proporcionar pruebas, soporte y mantenimiento.

5.7. El Proveedor mantendrá medidas diseñadas para evaluar, probar y aplicar parches de advertencia de seguridad a los Servicios y Entregables y sus sistemas, redes, aplicaciones y componentes subyacentes asociados en el ámbito de dichos Servicios y Entregables, así como los sistemas, redes, aplicaciones y componentes subyacentes utilizados en el Manejo de Tecnologías de Kyndryl. Tras determinar que un parche de advertencia de seguridad es aplicable y adecuado, el Proveedor implementará dicho parche conforme con las directrices documentadas de evaluación del riesgo y la gravedad. La implementación del Proveedor de parches de advertencia de seguridad estará sujeta a su política de gestión de cambios.

5.8. Si Kyndryl tiene una base razonable para considerar que el hardware o el software que el Proveedor proporciona a Kyndryl puede contener elementos intrusivos, como spyware, malware o código malicioso, el Proveedor cooperará oportunamente con Kyndryl en la investigación y solución de las sospechas de Kyndryl.

6. Aprovisionamiento de Servicio

6.1 El Proveedor dará soporte a los métodos comunes de autenticación federada del sector para cualquier cuenta de usuario o Cliente de Kyndryl, y el Proveedor seguirá las Prácticas Recomendadas del Sector en la autenticación de dichas cuentas de Usuario o Cliente de Kyndryl (como el inicio de sesión único de diversos factores de gestión centralizada de Kyndryl, utilizando OpenID Connect o SAML).

7. Subcontratistas. Sin limitación de las obligaciones del Proveedor o los derechos de Kyndryl bajo el Documento Transaccional o el acuerdo base asociado entre las partes con respecto a la retención de subcontratistas, el Proveedor se asegurará de que cualquier subcontratista que realice trabajos para el Proveedor haya instituido controles de gestión para cumplir los requisitos y obligaciones que estas Condiciones imponen al Proveedor.

8. Soportes Físicos. El Proveedor saneará de forma segura los soportes físicos para su reutilización antes de dicha reutilización y destruirá los soportes físicos que se van a reutilizar, de conformidad con las Prácticas Recomendadas del Sector para el saneamiento de soportes.

Artículo IX, Informes y Certificaciones de Servicios Alojados

Este Artículo se aplica si el Proveedor presta un Servicio Alojado a Kyndryl.

1.1 El Proveedor obtendrá las siguientes certificaciones o informes en los plazos que se definen a continuación:

Certificaciones / Informes	**Periodo de Tiempo**
En relación con los Servicios Alojados del Proveedor: Certificación de cumplimiento de la ISO 27001, Tecnologías de la información, Técnicas de seguridad, Sistemas de gestión de seguridad de la información, con dicha certificación basada en la evaluación de un auditor independiente reputado **O bien** SOC 2 de Tipo 2: un informe realizado por un auditor independiente reconocido que demuestre su revisión de los sistemas, controles y operaciones del Proveedor, de acuerdo con un SOC 2 de Tipo 2 (que incluya, como mínimo, seguridad, confidencialidad y disponibilidad)	El Proveedor deberá obtener la certificación ISO 27001 en un plazo de 120 días desde la fecha efectiva de este Documento Transaccional* o la Fecha de Asunción**, y renovar posteriormente la certificación en base a la evaluación de un auditor independiente de buena reputación cada 12 meses posteriores (donde cada renovación se realizará con la versión más actualizada del estándar) El Proveedor obtendrá el informe SOC 2 de Tipo 2 240 días después de la fecha efectiva del Documento Transaccional* o la Fecha de Asunción** y posteriormente obtendrá un nuevo informe de un auditor independiente de buena reputación que demuestre su revisión de los sistemas, controles y operaciones del Proveedor de conformidad con un SOC 2 de Tipo 2 (que incluya, como mínimo, seguridad, confidencialidad y disponibilidad) cada 12 meses posteriores * Si, a partir de la fecha efectiva, el Proveedor proporciona un Servicio Alojado ** La fecha en la que el Proveedor asume la obligación de proporcionar un Servicio Alojado

1.2 Si el Proveedor lo solicita por escrito, e Kyndryl lo aprueba por escrito, el Proveedor puede obtener una certificación o un informe sustancialmente equivalente a los mencionados anteriormente, bajo el supuesto de que los plazos establecidos en la tabla anterior se aplicarán sin cambios con respecto a la certificación o informe sustancialmente equivalente.

1.3 El Proveedor: (a) a petición, proporcionará rápidamente a Kyndryl una copia de cada certificación e informe que el Proveedor está obligado a obtener y (b) resolverá rápidamente cualquier debilidad de control interno observada durante el SOC 2 u otras revisiones sustancialmente equivalentes (si Kyndryl así lo aprueba).

Artículo X, Cooperación, Verificación y Remediación

Este artículo se aplica si el Proveedor proporciona algún Servicio o Entregable a Kyndryl.

1. Cooperación del Proveedor

1.1. 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, incluyendo 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.

1.2. Las partes acuerdan: (a) proporcionarse, a petición, entre sí dicha información adicional, (b) ejecutar y entregarse mutuamente cualquier otro tipo de documentación, y (c) llevar a cabo otras acciones, todo aquello que la otra parte pueda razonablemente solicitar con el fin de ejecutar la intencionalidad de estas Condiciones y los documentos mencionados en estas Condiciones. Por ejemplo, si Kyndryl lo solicita, el Proveedor proporcionará oportunamente las condiciones centradas en la privacidad y la seguridad de sus contratos escritos con Subencargados del Tratamiento y subcontratistas, incluyendo, cuando el Proveedor tenga derecho a hacerlo, la concesión de acceso a los contratos en sí.

1.3. Si Kyndryl lo solicita, el Proveedor proporcionará oportunamente información sobre los países donde se fabricaron, desarrollaron o obtuvieron de otro modo sus Entregables y los componentes de los Entregables.

2. Verificación (como se usa a continuación, "Instalación" significa una ubicación física donde el Proveedor aloja, procesa o accede a los Materiales de Kyndryl)

2.1. El Proveedor mantendrá un registro auditable que demuestre la conformidad con estas Condiciones.

2.2. Kyndryl, propiamente o mediante un auditor externo, puede, con 30 días de notificación previa por escrito al Proveedor, verificar la conformidad del Proveedor con estas Condiciones, incluyendo el acceso a cualquier Instalación o Instalaciones para tales fines, aunque Kyndryl no accederá a ningún centro de datos donde el Proveedor trate 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, incluyendo 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.

2.3. 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 una Brecha de Seguridad e Kyndryl quiera verificar el cumplimiento de las obligaciones relevantes para la infracción. En cualquier caso, Kyndryl proporcionará la misma notificación previa por escrito de 30 días como se especifica en el Apartado 2.2 anterior, pero la urgencia de abordar una Brecha de Seguridad puede requerir que Kyndryl realice una verificación con menos de 30 días de notificación previa por escrito.

2.4. Un regulador u otro Responsable del Tratamiento puede ejercer los mismos derechos que Kyndryl en los Apartados 2.2 y 2.3, bajo el supuesto de que un regulador puede ejercer cualquier derecho adicional que tenga según la legislación vigente.

2.5. 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.

3. Programa Contra la Falsificación

3.1. Si los Entregables del Proveedor incluyen componentes electrónicos (por ejemplo, unidades de disco duro, unidades de estado sólido, memoria, unidades centrales de procesamiento, dispositivos lógicos o

cables), el Proveedor mantendrá y seguirá un programa documentado de prevención de posibles falsificaciones para, en primer lugar, evitar que el Proveedor proporcione componentes falsificados a Kyndryl y, en segundo lugar, detectar y corregir de inmediato cualquier caso en que el Proveedor proporcione componentes falsificados por error a Kyndryl. El Proveedor impondrá esta misma obligación de mantener y seguir un programa documentado de prevención de posibles falsificaciones en todos sus proveedores que proporcionen componentes electrónicos incluidos en los Entregables del Proveedor a Kyndryl.

4. Remediación

4.1. Si el Proveedor no cumple con cualquiera de sus obligaciones bajo estas Condiciones, y esa anomalía causa una Brecha de Seguridad, el Proveedor corregirá la anomalía en su ejecución y corregirá el efecto nocivo de la Brecha de Seguridad, con dicho rendimiento y corrección bajo la dirección y una programación razonables de Kyndryl. Sin embargo, si la Infracción de Seguridad surge de la prestación del Proveedor de un Servicio alojado multiarrendatario y, en consecuencia, afecta a muchos clientes del Proveedor, incluida Kyndryl, el Proveedor, dada la naturaleza de la Infracción de Seguridad, corregirá oportuna y adecuadamente la anomalía en su rendimiento y remediará los efectos dañinos de la Infracción de Seguridad, al tiempo que brinda la debida consideración a cualquier opinión de Kyndryl sobre dichas correcciones y remediación.

4.2. Kyndryl tendrá derecho a participar en la remediación de cualquier Infracción de Seguridad a la que se haga referencia en la Sección 4.1, según lo crea conveniente o necesario, y el Proveedor será responsable de sus costes y gastos para la corrección de su rendimiento y de los costes y gastos de remediación en que incurran las partes con respeto a dicha Infracción de Seguridad.

4.3. A modo de ejemplo, los costes y gastos de corrección asociados con una Brecha de Seguridad podrían incluir los derivados de detectar e investigar una Brecha de Seguridad, determinar las responsabilidades bajo la legislación y las normativas aplicables, proporcionar notificaciones de incumplimiento, establecer y mantener centros de atención telefónica, prestar Servicios de supervisión y restauración de crédito, recargar datos, corregir defectos del producto (incluyendo a través del Código Fuente u otros desarrollos), retener a terceros para ayudar con las actividades anteriores u otras actividades relevantes, y otros costes y gastos que sean necesarios para corregir los efectos nocivos de la Brecha de Seguridad. Para mayor claridad, los costes y gastos de corrección no incluirían la pérdida de ganancias, negocios, valor, ingresos, previsiones o ahorros anticipados de Kyndryl.