Artículo I, Información de contacto comercial

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 cuando hagan negocios en relación con la entrega de Servicios y Productos del Proveedor.

1.2 Una parte:

(a) no usará ni revelará la BCI de la otra parte para ningún otro fin (para mayor claridad, ninguna de las partes venderá la BCI de la otra parte ni revelará o usará la BCI de la otra parte para fines de marketing sin la autorización previa por escrito de la otra parte y, cuando sea necesario, la autorización previa por escrito de los Interesados afectados), y

(b) suprimirá, modificará, corregirá, devolverá, proporcionará información sobre el Tratamiento, restringirá el Tratamiento, o tomará cualquier otra acción razonablemente solicitada con respecto a la BCI de la otra parte sin demora previa solicitud por escrito de la otra parte, siempre que se produzca un uso no autorizado de la información personal, y la parte desea detener el tratamiento y aplicar medidas correctoras.

1.3 Las partes no establecen una relación de Responsable conjunto con respecto a la BCI de la otra parte y no suministrar el Documento de transacción se considerará o se interpretará como una indicación de intento de establecer una relación de Responsable conjunto.

1.4 La Declaración de privacidad de Kyndryl en https://www.kyndryl.com/us/en/privacy contiene detalles adicionales sobre el Tratamiento de la BCI de Kyndryl.

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

1.6 El Proveedor avisará a Kyndryl inmediatamente (y en cualquier caso antes de 48 horas) después de conocer cualquier Vulneración de seguridad que involucre la BCI de Kyndryl. El Proveedor enviará dicha notificación a cyber.incidents@kyndryl.com. El Proveedor proporcionará a Kyndryl la información solicitada de forma razonable sobre dicha vulneración y el estado de cualquier actividad de corrección y restauración por parte del Proveedor. A modo de ejemplo, la información solicitada de forma razonable puede incluir registros que demuestren el 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 en que sean relevantes para la vulneración o las actividades de corrección 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 corrección) son los únicos Artículos que se aplican a dicho Tratamiento.

Artículo II, Medidas técnicas y organizativas, Seguridad de los datos

Este Artículo se aplica si el Proveedor Trata Datos de Kyndryl distintos de la BCI de Kyndryl. El Proveedor cumplirá los requisitos de este Artículo al proporcionar todos los Servicios y Productos y, al hacerlo, protegerá los Datos de Kyndryl contra la pérdida, destrucción, alteración, divulgación accidental o no autorizada, acceso sin autorización y formas de Tratamiento ilegales. Los requisitos de este Artículo se extienden a todas las aplicaciones, plataformas e infraestructura de TI que el Proveedor utilice o administre para proporcionar los Productos y Servicios, incluidos todos los entornos de desarrollo, prueba, alojamiento, soporte, operaciones y centro 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 ni datos, incluidos Datos personales, sin la autorización previa por escrito de Kyndryl, y el Proveedor no puede utilizar los Datos de Kyndryl de ninguna forma, agregados o de otro modo, para ningún otro propósito que no sea proporcionar Servicios y Productos (por ejemplo, el Proveedor no tiene permitido utilizar ni reutilizar los Datos de Kyndryl para evaluar la efectividad ni como medio para mejorar las ofertas del Proveedor, para investigación y desarrollo, para crear nuevas ofertas ni para generar informes sobre las ofertas del Proveedor). A menos que se permita expresamente en el Documento de transacción, el Proveedor tiene prohibido Vender los Datos de Kyndryl.

1.2 El Proveedor no podrá incorporar ninguna tecnología de rastreo web en los Productos ni como parte de los Servicios (estas tecnologías incluyen HTML5, almacenamiento local, etiquetas o señales de terceros y balizas web) a menos que se permita expresamente en el Documento de transacción.

2. Solicitudes de terceros y Confidencialidad

2.1 El Proveedor no revelará los Datos de Kyndryl a ningún tercero, a menos que Kyndryl lo autorice previamente por escrito. Si un gobierno, incluido cualquier regulador, exige el acceso a los datos de Kyndryl (p. ej., si el gobierno de los EE. UU. envía una orden de seguridad nacional al Proveedor para obtener datos de Kyndryl), o si se requiere una divulgación de los datos de Kyndryl por ley, el Proveedor avisará a Kyndryl por escrito de dicha demanda o requerimiento y dará a Kyndryl una oportunidad razonable para oponerse a cualquier divulgación (cuando la ley prohíba la notificación, el Proveedor tomará las medidas que considere razonablemente apropiadas para oponerse a la prohibición y divulgación de los Datos de Kyndryl a través de una acción legal u otros medios).

2.2 El Proveedor garantiza a Kyndryl que: (a) solo aquellos de sus empleados que necesiten acceder a los Datos de Kyndryl para proporcionar Servicios o Productos tendrán dicho acceso, y solo en la medida necesaria para proporcionar esos Servicios y Productos; 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.

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 cuando se rescinda o venza el Documento de transacción, o antes a petición de Kyndryl. Si Kyndryl solicita suprimir los datos, entonces el Proveedor, de conformidad con las Mejores prácticas del sector, hará que los datos queden ilegibles y no puedan recomponerse ni reconstruirse, y certificará la eliminación a Kyndryl. Si Kyndryl solicita la devolución de los Datos de Kyndryl, el Proveedor lo hará según el plazo 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 para Tratar los Datos Personales de Kyndryl con el único propósito de proporcionar los Productos y Servicios de acuerdo con las instrucciones de Kyndryl, incluidas las contenidas en estos Términos, el Documento de transacción y el acuerdo base asociado entre las partes. Si el Proveedor no cumple alguna instrucción, Kyndryl podrá rescindir la parte afectada de los Servicios mediante un aviso 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. Si el Proveedor incumple alguna de sus obligaciones en virtud de estos Términos y dicho incumplimiento provoca un uso no autorizado de la Información personal o, en general, en cualquier caso de uso no autorizado de la Información personal, Kyndryl tendrá derecho a detener el tratamiento, corregir el error y subsanar los efectos nocivos del uso no autorizado. Dichas actividades correctivas se realizarán en los plazos y según las instrucciones razonables de Kyndryl.

1.2 El Proveedor respetará todas las leyes protección de datos aplicables a los Servicios y Productos.

1.3 Un Anexo al Documento de transacción, o el propio Documento de transacción, 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 del Tratamiento; y
(e) una lista de Subencargados.

2. Medidas técnicas y organizativas

2.1 El Proveedor implementará y mantendrá las medidas técnicas y organizativas definidas en el Artículo II (Medidas técnicas y organizativas, Seguridad de los datos) y el Artículo VIII (Medidas técnicas y organizativas, Seguridad general) y, al hacerlo, garantizará un nivel de seguridad adecuado al riesgo que presentan sus Servicios y Productos. El Proveedor certifica y comprende las restricciones del Artículo II, este Artículo III y el Artículo VIII y se compromete a cumplirlas.

3. Derechos y solicitudes de los Interesados

3.1 El Proveedor informará a Kyndryl sin demora (en un plazo que permita a Kyndryl y a cualquier Otro responsable cumplir sus obligaciones legales) de cualquier solicitud de un Interesado para 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 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.

3.2 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 solicite Kyndryl, en un plazo que permita a Kyndryl responder oportunamente a dichos Otros responsables o terceros.

4. Subencargados

4.1 El Proveedor proporcionará a Kyndryl un aviso previo por escrito antes de contratar a un nuevo Subencargado o de ampliar el alcance del Tratamiento por parte de un Subencargado existente. En dicho aviso

por escrito se identificará el nombre del Subencargado y se describirá el alcance nuevo o ampliado del Tratamiento. Kyndryl puede oponerse a la contratación del nuevo Subencargado o a la ampliación del alcance por motivos razonables en cualquier momento y, si lo hace, las partes colaborarán de buena fe para atender la objeción de Kyndryl. Sin perjuicio del derecho de Kyndryl a oponerse en cualquier momento, el Proveedor puede contratar al nuevo Subencargado o ampliar el alcance del Tratamiento del Subencargado existente si Kyndryl no ha presentado ninguna objeción en un plazo de 30 días a partir de la fecha del aviso por escrito del Proveedor.

4.2 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 Trate cualquier Dato de Kyndryl. El Proveedor es completamente responsable ante Kyndryl por el cumplimiento de las obligaciones de cada Subencargado.

5. Tratamiento transfronterizo de datos

Como se usa a continuación:

País adecuado significa un país que proporciona un nivel adecuado de protección de datos con respecto a la transferencia relevante de conformidad con las leyes de protección de datos aplicables o las decisiones de los reguladores.

Importador de datos significa un Encargado o un Subencargado que no está establecido en un País adecuado.

Cláusulas contractuales tipo de la UE («SCC de la UE») significa las Cláusulas contractuales tipo de la UE (Decisión 2021/914 de la Comisión) con cláusulas opcionales aplicadas excepto la opción 1 de la Cláusula 9(a) y la opción 2 de la Cláusula 17, tal como se publica oficialmente en https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

Cláusulas contractuales tipo serbias («SCC serbias») significa las Cláusulas contractuales tipo serbias tal como fueron adoptadas por el «Comisionado serbio para la información de importancia pública y la protección de datos personales», publicadas en https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Cláusulas contractuales tipo («**SCC**») significa 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 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 (tampoco mediante acceso remoto) ningún Dato personal de Kyndryl entre fronteras sin la autorización previa por escrito de Kyndryl. Si Kyndryl proporciona dicha autorización, las partes cooperarán para garantizar el cumplimiento de las leyes de protección de datos aplicables. Si dichas leyes exigen las SCC, el Proveedor suscribirá las SCC de inmediato a petición de Kyndryl.

5.2 Acerca de las SCC de la UE:

(a) Si el Proveedor no está establecido en un País adecuado: el proveedor suscribe las SCC de la UE como Importador de datos con Kyndryl, y el Proveedor celebrará acuerdos por escrito con cada Subencargado aprobado, de conformidad con la Cláusula 9 de las SCC de la UE, y proporcionará a Kyndryl copias de esos acuerdos previa solicitud.

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

(ii) El Módulo 2 de las SCC de la UE se aplica cuando Kyndryl es un Responsable y el Módulo 3 se aplica cuando Kyndryl es un Encargado. De conformidad con la Cláusula 13 de las SCC de la UE, cuando se apliquen los Módulos 2 o 3, las partes acuerdan que (1) las SCC de la UE se regirán por la ley del estado miembro de la UE donde se encuentra la autoridad de control competente y (2) cualquier disputa que surja de las SCC de la UE se llevará ante los tribunales del estado miembro de la UE donde se encuentre la autoridad de control competente. Si la ley en (1) no permite derechos a favor de terceros, entonces las SCC de la UE se regirán por la ley de los Países Bajos y cualquier disputa que surja de las SCC de la UE en virtud de (2) se resolverá ante el tribunal de Ámsterdam en los Países Bajos.

(b) Si ambas partes, tanto el Proveedor como Kyndryl, están establecidas en un País adecuado, el Proveedor actuará como Exportador de datos y participará en las SCC de la UE con cada Subencargado aprobado en un País no adecuado. El Proveedor realizará la Evaluación del impacto de la transferencia (TIA) requerida y avisará a Kyndryl sin dilación indebida sobre (1) cualquier necesidad de aplicar medidas complementarias y (2) las medidas aplicadas. Previa solicitud, el Proveedor proporcionará los resultados de la TIA y cualquier información necesaria para comprender y evaluar los resultados a Kyndryl. En caso de que Kyndryl no esté de acuerdo con los resultados de la TIA de los Proveedores o con las medidas complementarias aplicadas, Kyndryl y el Proveedor trabajarán juntos para encontrar una solución viable. Kyndryl mantiene el derecho de suspender o rescindir los servicios de los Proveedores en cuestión sin indemnización. Para evitar dudas, esto no exime a los Subencargados del Proveedor de la obligación de suscribir las SCC de la UE con Kyndryl o sus Clientes, como se describe en la sección 5.2 (d) a continuación.

(c) Si el Proveedor está establecido en el Espacio Económico Europeo y Kyndryl es un Responsable no sujeto al Reglamento General de Protección de Datos 2016/679, entonces se aplica el Módulo 4 de las SCC de la UE, y el Proveedor suscribe 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 ley de los Países Bajos y cualquier disputa que surja de las SCC de la UE se resolverá ante el tribunal de Ámsterdam en los Países Bajos.

(d) Si Otros responsables, como Clientes o afiliados, solicitan convertirse en parte de las SCC de la UE de conformidad con la «cláusula de adhesión» de la Cláusula 7, el Proveedor acepta dicha solicitud.

(e) Las Medidas técnicas y organizativas requeridas para completar el Anexo II de las SCC de la UE se pueden encontrar en estos Términos, el propio Documento de transacción y el acuerdo base asociado entre las partes.

(f) En caso de conflicto entre las SCC de la UE y estos Términos, prevalecerán las SCC de la UE.

5.3 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 estos Términos, prevalecerán los Anexos del Reino Unido.

5.4 Acerca de las SCC serbias:

(a) Si el Proveedor no está establecido en un País adecuado: (i) el Proveedor suscribe las SCC serbias con Kyndryl en nombre del propio Proveedor como Encargado; y (ii) el Proveedor suscribirá acuerdos por escrito con cada Subencargado aprobado, de conformidad con el Artículo 8 de las SCC serbias, y proporcionará a Kyndryl copias de dichos acuerdos a petición.

(b) Si el Proveedor está establecido en un País adecuado, entonces el Proveedor suscribe las SCC serbias con Kyndryl en nombre de cada Subencargado ubicado en un País no adecuado. Si el Proveedor no puede hacerlo para dicho Subencargado, entonces el Proveedor proporcionará a Kyndryl las SCC serbias suscritas por dicho Subencargado para la contrafirma de Kyndryl antes de permitir que el Subencargado Trate los Datos personales de Kyndryl.

(c) Las SCC serbias entre Kyndryl y el Proveedor servirán como SCC serbias entre un Responsable y un Encargado o como un acuerdo recíproco por escrito entre el «encargado» y el «subencargado», según lo requieran los hechos. En caso de conflicto entre las SCC serbias y estos Términos, prevalecerán las SCC serbias.

(d) La información necesaria para completar los Apéndices 1 a 8 de las SCC serbias con el fin de regular la transferencia de Datos personales a un País no adecuado se puede encontrar en estos Términos y en el Anexo del Documento de transacción, o en el propio Documento de transacción.

5.5. 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 asistirá a Kyndryl con las medidas técnicas y organizativas apropiadas para cumplir con las obligaciones asociadas con las solicitudes y derechos del Interesado. El Proveedor también asistirá a Kyndryl para garantizar el cumplimiento de conformidad con las obligaciones relativas a la seguridad del Tratamiento, la notificación y comunicación de una Vulneración de seguridad y la creación de evaluaciones de impacto de protección de datos , incluida la consulta previa con el regulador responsable, si se requiere, teniendo en cuenta la información disponible para el Proveedor.

6.2 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.

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 con los requisitos de este Artículo y, al hacerlo, protegerá el Código fuente de Kyndryl contra la pérdida, destrucción, alteración, divulgación accidental o no autorizada, acceso sin autorización y formas ilegales de Manejo. Los requisitos de este Artículo se extienden a todas las aplicaciones, plataformas e infraestructura de TI que el Proveedor utilice o gestione para proporcionar los Productos y Servicios, incluidos todos los entornos de desarrollo, prueba, alojamiento, soporte, operaciones y centro de datos.

1. Requerimientos de seguridad

Como se usa a continuación,

País prohibido significa cualquier país: (a) que el gobierno de los EE. UU. haya designado como adversario extranjero en virtud de la Orden ejecutiva del 15 de mayo de 2019 sobre la seguridad de las tecnologías de información y comunicaciones y la cadena de suministro de servicios, (b) enumerado de conformidad con la Sección 1654 de Ley de Autorización de Defensa Nacional estadounidense de 2019, o (c) identificado como un «País prohibido» en el Documento de transacción.

1.1 El Proveedor no distribuirá ni colocará ningún Código fuente de Kyndryl en custodia en beneficio de ningún tercero.

1.2 El Proveedor no permitirá que ningún Código fuente de Kyndryl esté alojado en servidores ubicados en un País prohibido. El Proveedor no permitirá a nadie, incluido su Personal, que se encuentre o que visite un País prohibido (durante dicha visita), por cualquier motivo, acceder o usar cualquier Código fuente de Kyndryl, con independencia del lugar del mundo en que se encuentre ese Código fuente de Kyndryl, y el Proveedor no permitirá que se realice ningún desarrollo, prueba u otro trabajo en un País prohibido que requiera dicho acceso o uso.

1.3 El Proveedor no colocará ni distribuirá el Código fuente de Kyndryl en ninguna jurisdicción donde la ley o la interpretación de la ley requieran la divulgación del Código fuente a un tercero. Si hay un cambio de ley o interpretación de ley en una jurisdicción donde se encuentre el Código fuente de Kyndryl que pueda motivar que el Proveedor deba revelar dicho Código fuente a un tercero, el Proveedor destruirá o eliminará inmediatamente dicho Código fuente de dicha jurisdicción, y no colocará ningún Código fuente de Kyndryl adicional en dicha jurisdicción mientras dicha ley o interpretación de la ley permanezca operativa.

1.4 El Proveedor no realizará, directa ni indirectamente, ninguna acción, incluida la firma de cualquier acuerdo, que haga que el Proveedor, Kyndryl o cualquier tercero incurra en una obligación de divulgación en virtud de las Secciones 1654 o 1655 de la Ley de Autorización de Defensa Nacional estadounidense de 2019. Para mayor claridad, salvo que se permita expresamente en el Documento de transacción o en el acuerdo base asociado entre las partes, el Proveedor no puede revelar el Código fuente de Kyndryl a terceros, bajo ninguna circunstancia, sin la autorización previa 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 sea llevado a un País prohibido o cualquier jurisdicción sujeta a la Sección 1.3 anterior, (b) el Proveedor ha publicado, accedido o utilizado de otro modo el Código fuente de Kyndryl de una manera no permitida por el Documento de transacción, el acuerdo base asociado u otro acuerdo entre las partes o (c) el Proveedor ha incumplido la Sección 1.4 anterior, entonces sin limitar los derechos legales de Kyndryl a tratar dicho incumplimiento en derecho o equidad bajo el Documento de transacción, el acuerdo base asociado u otro acuerdo entre las partes: (i) si dicha notificación es para el Proveedor, el Proveedor compartirá la notificación de inmediato con Kyndryl; y (ii) el Proveedor, siguiendo las instrucciones razonables de Kyndryl, investigará y solucionará el asunto en el plazo que Kyndryl determine razonablemente (después de consultar con el Proveedor).

1.6 Si Kyndryl cree razonablemente que pueden ser necesario incorporar 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, sin dichos cambios, pueda impedirse a Kyndryl que venda a ciertos Clientes o en ciertos mercados o que no pueda

satisfacer los requisitos de seguridad del Cliente o de la cadena de suministro), entonces Kyndryl puede comunicarse con el Proveedor para analizar las acciones necesarias para mitigar dichos riesgos, incluida la incorporación de cambios en dichas políticas, procedimientos, controles o prácticas. A petición de Kyndryl, el Proveedor cooperará con Kyndryl para evaluar si dichos cambios son necesarios y para implementar los cambios apropiados y acordados mutuamente.

Artículo V, Desarrollo seguro

Este Artículo se aplica si el Proveedor proporcionará su propio Código fuente, el de terceros o Software local a Kyndryl, o se proporcionará alguno de los Productos o Servicios del Proveedor a un Cliente de Kyndryl como parte de un producto o servicio de Kyndryl.

1. Preparación de seguridad

1.1 El Proveedor cooperará con los procesos internos de Kyndryl que evalúan la disponibilidad de seguridad de los productos y servicios de Kyndryl que dependen de cualquiera de los Productos del Proveedor, incluso respondiendo de manera oportuna y completa a las solicitudes de información, ya sea a través de documentos, otros registros, entrevistas con el Personal relevante del Proveedor 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 de transacción de conformidad con las Mejores prácticas del sector las redes, plataformas, sistemas, aplicaciones, dispositivos, infraestructura física, respuesta a incidencias, así como las políticas, procedimientos y controles de seguridad centrados en el Personal que sean necesarios para proteger: (a) los sistemas y entornos de desarrollo, construcción, pruebas y operaciones que el Proveedor o cualquier tercero contratado por el Proveedor opere, administre, utilice o emplee para o en relación con los Productos y (b) todo el código fuente de los Productos contra pérdida, formas de manejo ilícitas, y acceso sin autorización, divulgación o alteración.

3. Certificación ISO 20243

3.1 Esta Sección 3 solo se aplica si cualquiera de los Productos o Servicios del Proveedor se proporcionarán 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 alterados y falsificados maliciosamente (ya sea una certificación autoevaluada o basada en la evaluación de un auditor acreditado independiente). Como alternativa, si el Proveedor lo solicita por escrito y Kyndryl lo aprueba por escrito, el Proveedor obtendrá una certificación de conformidad con un estándar del sector que aborde las prácticas seguras de desarrollo y cadena de suministro sustancialmente equivalente (ya sea una certificación autoevaluada o una basada en la evaluación de un auditor independiente acreditado, si Kyndryl lo aprueba).

3.3 El Proveedor obtendrá la certificación de conformidad con la norma ISO 20243 o un estándar del sector sustancialmente equivalente (si Kyndryl lo aprueba por escrito) antes de 180 días después de la fecha de vigencia del Documento de transacción
y después renovará la certificación cada 12 meses (cada renovación con arreglo a la versión más reciente de la norma aplicable en ese momento, es decir, ISO 20243 o, cuando Kyndryl lo haya aprobado por escrito, una norma industrial sustancialmente equivalente que aborde el desarrollo seguro y las prácticas de la cadena de suministro).

3.4 El Proveedor, previa solicitud, proporcionará de inmediato a Kyndryl una copia de las certificaciones que el Proveedor está obligado a obtener, según las Secciones 2.1 y 2.2 anteriores.

4. Vulnerabilidades de seguridad

Como se usa a continuación,

Corrección de errores significa correcciones de errores y revisiones que corrijan errores o deficiencias, incluidas Vulnerabilidades de seguridad, en los Productos.

Mitigación significa cualquier medio conocido de reducir o evitar los riesgos de una Vulnerabilidad de seguridad.

Vulnerabilidad de seguridad significa un estado en el diseño, codificación, desarrollo, implementación, prueba, operación, soporte, mantenimiento o gestión de un Producto o Servicio que permita un ataque por cualquier persona que pueda dar lugar a un acceso sin autorización o explotación, incluyendo: (a) acceder a, controlar o interrumpir el funcionamiento de un sistema, (b) acceder a, borrar, alterar o extraer datos o (c) cambios de identidad, autorizaciones o permisos de usuarios o administradores. Una Vulnerabilidad de seguridad puede existir independientemente de que se le haya asignado un ID de Vulnerabilidades y exposiciones comunes (CVE) o cualquier puntuación o clasificación oficial.

4.1 El Proveedor declara y garantiza que: (a) sigue las Mejores prácticas del sector para identificar las Vulnerabilidades de seguridad, incluido a través del escaneo continuo de la seguridad estática y dinámica del código fuente de las aplicaciones, del escaneo de la seguridad del código abierto y del escaneo de las vulnerabilidades del sistema, y (b) cumple con los requisitos de estos Términos para ayudar a impedir, detectar y corregir Vulnerabilidades de seguridad en los Productos y en todas las aplicaciones de TI, plataformas e infraestructura en y a través de las cuales el Proveedor crea y proporciona Servicios y Productos.

4.2 Si el Proveedor tiene conocimiento de una Vulnerabilidad de seguridad en un Producto o en cualquier aplicación , plataforma o infraestructura de TI, el Proveedor proporcionará a Kyndryl una Corrección de errores y mitigaciones para todas las versiones y ediciones de los Productos de acuerdo con los Niveles de gravedad y los plazos de tiempo definidos en las siguientes tablas:

Nivel de gravedad*
Vulnerabilidad de seguridad de emergencia: es una Vulnerabilidad de seguridad que constituye una amenaza grave y potencialmente global. Kyndryl designa las Vulnerabilidades de seguridad de emergencia bajo su discreción exclusiva, independientemente de la puntuación base de CVSS.
Crítica: es una Vulnerabilidad de seguridad que tiene una puntuación base de CVSS comprendida entre 9 y 10,0
Alta: es una Vulnerabilidad de seguridad que tiene una puntuación base de CVSS comprendida entre 7,0 y 8,9
Media: es una Vulnerabilidad de seguridad que tiene una puntuación base de CVSS comprendida entre 4,0 y 6,9
Baja: es una Vulnerabilidad de seguridad que tiene una puntuación base de CVSS comprendida entre 0,0 y 3,9

Plazos de tiempo				
Emergencia	***Crítica***	***Alta***	***Media***	***Baja***
4 días o menos, según determine la Oficina principal de seguridad de la información de Kyndryl	30 días	30 días	90 días	Según las Mejores prácticas del sector

* En cualquier caso, cuando no sea posible asignar fácilmente una puntuación base de CVSS a una Vulnerabilidad de seguridad, el Proveedor aplicará un Nivel de gravedad que sea apropiado para la naturaleza y las circunstancias de dicha vulnerabilidad.

4.3 Para una Vulnerabilidad de seguridad que se haya divulgado públicamente y para la cual el Proveedor

aún no haya proporcionado ninguna corrección o mitigación de errores a Kyndryl, el Proveedor implementará cualquier control de seguridad adicional técnicamente factible que pueda 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 Producto o cualquier aplicación, plataforma o infraestructura antes mencionada, entonces, sin perjuicio de cualquier otro derecho de Kyndryl, el Proveedor tomará las medidas necesarias para que Kyndryl discuta sus inquietudes directamente con un Vicepresidente del Proveedor o un directivo equivalente que sea responsable de entregar la Corrección de errores.

4.5 Algunos ejemplos de Vulnerabilidades de seguridad incluyen código de terceros o código fuente de terceros al final de su vida útil (EOS), donde estos tipos de código ya no reciben correcciones de seguridad.

Artículo VI, Acceso a sistemas corporativos

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

1. Términos 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 acceso cumplan con los requisitos de este Artículo.

1.2 Kyndryl identificará los medios por los cuales los empleados del Proveedor pueden acceder a los Sistemas corporativos, incluido si dichos empleados accederán a los Sistemas corporativos a través de Dispositivos proporcionados por el Proveedor o por Kyndryl.

1.3 Los empleados del Proveedor solo podrán acceder a los Sistemas corporativos, y solo podrán utilizar los Dispositivos que Kyndryl autorice para ese acceso, para prestar los Servicios. Los empleados del Proveedor no pueden utilizar los Dispositivos que Kyndryl autorice 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.

1.4 Para mayor claridad, los empleados del Proveedor no pueden usar los Dispositivos que Kyndryl autorice para acceder a los Sistemas corporativos por ninguna razón 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 motivos personales).

1.5 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).

1.6 Previa solicitud, 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 periodo de tiempo que Kyndryl identifique.

1.7 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: (a) ser empleado del Proveedor o (b) 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.

1.8 El Proveedor informará inmediatamente a Kyndryl de cualquier incidencia de seguridad real o sospechada (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.

1.9 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, entonces el Proveedor confirmará contractualmente que esas personas y sus empleadores cumplen con los requisitos de este Artículo como si esas personas fueran empleados del Proveedor, y será responsable ante Kyndryl por todas las acciones y omisiones de dicha persona o empleador con respecto al acceso a dicho Sistema corporativo.

2. Software del dispositivo

2.1 El Proveedor indicará a sus empleados que instalen oportunamente cualquier software del Dispositivo que Kyndryl requiera para facilitar el acceso a los Sistemas corporativos de manera segura. Ni el Proveedor ni sus empleados interferirán con las operaciones de ese software ni con las características de seguridad que el software habilita.

2.2 El proveedor y sus empleados cumplirán las normas de configuración de dispositivos que establezca Kyndryl y colaborarán con Kyndryl para 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.

2.3 Los empleados del Proveedor no podrán compartir los Dispositivos que usen para acceder a los Sistemas corporativos, ni los nombres de usuario, contraseñas, o similares de sus Dispositivos, con ninguna otra persona.

2.4 Si Kyndryl autoriza a los empleados del Proveedor a acceder a los Sistemas corporativos utilizando los Dispositivos del Proveedor, entonces 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 Kyndryl así lo indique.

3. Supervisión y cooperación

3.1 Kyndryl tiene los derechos incondicionales de supervisar y 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, (a) realizar pruebas de seguridad en cualquier Dispositivo, (b) 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), registros, archivos y otros elementos almacenados en cualquier Dispositivo o transmitidos a través de cualquier Sistema corporativo, y (c) obtener una imagen forense completa de cualquier Dispositivo. Si Kyndryl necesita la cooperación del Proveedor para ejercer sus derechos, el Proveedor satisfará completa y oportunamente las solicitudes de Kyndryl para dicha cooperación (incluidas, por ejemplo, solicitudes para configurar de forma segura cualquier Dispositivo, instalar software de supervisión u otro en cualquier Dispositivo, 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 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 necesidad de avisar previamente al Proveedor ni a ningún empleado del Proveedor ni a otros, si Kyndryl lo considera necesario para proteger a Kyndryl.

3.3 Los derechos de Kyndryl no están bloqueados, disminuidos o restringidos de 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. Dispositivos de Kyndryl

4.1 Kyndryl mantendrá la propiedad de todos los Dispositivos de Kyndryl, y el Proveedor asumirá el riesgo de pérdida de los Dispositivos, 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.

4.2 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 las Mejores prácticas 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 se le entregaron, aparte del desgaste razonable, corriendo con los gastos hasta el lugar que Kyndryl indique. El incumplimiento por parte del Proveedor de cualquier obligación en esta Sección 4.2 constituye un incumplimiento material del Documento de transacción, del acuerdo base asociado y de cualquier acuerdo relacionado entre las partes, entendiendo 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.

4.3 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.

4.4. 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.

5. Actualizaciones

5.1 Sin perjuicio de cualquier disposición contraria en el Documento de transacción o en el acuerdo base asociado entre las partes, previo aviso por escrito al Proveedor y sin necesidad de obtener la autorización del Proveedor, Kyndryl puede actualizar, complementar o modificar este Artículo para abordar cualquier requisito de la legislación aplicable u obligación del Cliente, para reflejar cualquier desarrollo en las mejores prácticas de seguridad o de cualquier otro modo que Kyndryl considere necesario para proteger los Sistemas corporativos o a Kyndryl.

Artículo VII, Aumento de personal

Este artículo se aplicará cuando los empleados del Proveedor dediquen todo su tiempo de trabajo a prestar Servicios para Kyndryl, realicen todos esos Servicios en las instalaciones de Kyndryl, en las instalaciones del Cliente o desde sus hogares, y solo presten Servicios utilizando Dispositivos de Kyndryl para acceder a los Sistemas corporativos.

1. Acceso a los Sistemas corporativos y Entornos de Kyndryl

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

1.2 El Proveedor cumplirá con los términos establecidos 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 ser utilizados por el Proveedor y sus empleados para prestar Servicios. Para mayor claridad, en ningún caso el Proveedor ni sus empleados pueden usar cualquier otro dispositivo para prestar Servicios ni usar los Dispositivos de Kyndryl para cualquier otro cliente del Proveedor ni para cualquier otro propósito que no sea prestar Servicios a Kyndryl.

1.4 Los empleados del Proveedor que utilicen los Dispositivos de Kyndryl pueden intercambiar 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 con respecto a dicho almacenamiento en los Dispositivos de Kyndryl, en ningún caso el Proveedor ni sus empleados podrán eliminar los Materiales de Kyndryl de los repositorios, entornos, herramientas o infraestructura de Kyndryl donde Kyndryl los mantiene.

1.6 Para mayor claridad, el Proveedor y sus empleados no están autorizados a transferir ningún Material de Kyndryl a ningún repositorio, entorno, herramientas o infraestructura del Proveedor, ni a ningún otro sistema, plataforma, red o similares del Proveedor, sin la autorización previa por escrito de Kyndryl.

1.7 El Artículo VIII (Medidas técnicas y organizativas, Seguridad general) no se aplica a los Servicios del Proveedor donde los empleados del Proveedor dedicarán todo su tiempo de trabajo a prestar Servicios para Kyndryl, realizarán todos esos Servicios en las instalaciones de Kyndryl, las instalaciones del Cliente o desde sus hogares, y solo prestarán Servicios utilizando los Dispositivos de Kyndryl para acceder a los Sistemas corporativos. Por lo demás, 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 cualquier Servicio o Producto a Kyndryl, a menos que el Proveedor solo tenga acceso a la BCI de Kyndryl al proporcionar dichos Servicios y Productos (es decir, el Proveedor no Tratará ningún otro Dato de Kyndryl ni tendrá acceso a ningún otro Material de Kyndryl ni a ningún Sistema Corporativo), los únicos Servicios y Productos del Proveedor consistan en proporcionar Software local a Kyndryl, o el Proveedor proporcione todos sus Servicios y Productos en un modelo de aumento de personal de conformidad con el artículo VII, incluida la Sección 1.7 del mismo.

El Proveedor cumplirá con los requisitos de este Artículo y, al hacerlo, protegerá: (a) los Materiales de Kyndryl contra cualquier pérdida, destrucción, alteración, divulgación accidental o no autorizada, y acceso sin autorización, (b) los Datos de Kyndryl contra formas de Tratamiento ilegales y (c) la Tecnología de Kyndryl contra formas de Manejo ilegales. Los requisitos de este Artículo se extienden a todas las aplicaciones, plataformas e infraestructura de TI que el Proveedor utilice o gestione para proporcionar los Productos y Servicios, incluidos todos los entornos de desarrollo, prueba, alojamiento, soporte, operaciones y centro de datos.

1. Políticas de seguridad

1.1 El Proveedor mantendrá y seguirá las políticas y prácticas de seguridad TI que son parte integral del negocio del Proveedor, obligatorias para todo el Personal del Proveedor y coherentes con las Mejores prácticas del sector.

1.2 El Proveedor revisará sus políticas y prácticas de seguridad TI al menos una vez al año y las modificará según considere necesario para proteger los Materiales de Kyndryl.

1.3 El Proveedor mantendrá y seguirá los requisitos estándares de verificación laboral obligatorios para todos los nuevo empleados contratados, y extenderá dichos requisitos a todo el Personal del Proveedor y las subsidiarias del Proveedor en propiedad absoluta. Esos requisitos incluirán comprobaciones de antecedentes penales en la medida permitida por las leyes locales, pruebas de validación de identidad y verificaciones adicionales que el Proveedor considere necesarias. El Proveedor repetirá y revalidará periódicamente estos requisitos, según considere necesario.

1.4 El Proveedor impartirá formación sobre seguridad y privacidad a sus empleados anualmente y requerirá que todos esos empleados certifiquen cada año que cumplen con las políticas de conducta comercial ética, confidencialidad y seguridad del Proveedor, como se define en el código de conducta del Proveedor o documentos similares. El Proveedor impartirá formación adicional sobre políticas y procesos a las personas con acceso administrativo a cualquiera de los componentes de los Servicios, Productos o Materiales de Kyndryl. Dicha formación será específica para su función y el soporte de los Servicios, Productos y Materiales de Kyndryl, según sea necesario para mantener la conformidad y las certificaciones requeridas.

1.5 El Proveedor diseñará medidas de seguridad y privacidad para proteger y mantener la disponibilidad de los Materiales de Kyndryl, incluido a través de su implementación, mantenimiento y conformidad con políticas y procedimientos que requieran seguridad y privacidad por diseño, ingeniería segura y operaciones seguras, para todos los Servicios y Productos, y para todo el manejo de la Tecnología de Kyndryl.

2. Incidencias de seguridad

2.1 El Proveedor mantendrá y seguirá las políticas de respuesta a incidencias documentadas de forma coherente con las Mejores prácticas del sector para el manejo de incidencias de seguridad informática.

2.2 El Proveedor investigará el acceso o el uso no autorizados de los materiales de Kyndryl y definirá y ejecutará un plan de respuesta apropiado.

2.3 El Proveedor avisará a Kyndryl inmediatamente (y en ningún caso más tarde de 48 horas) tras conocer cualquier Vulneración de seguridad. El Proveedor enviará dicha notificación a cyber.incidents@kyndryl.com. El Proveedor proporcionará a Kyndryl la información solicitada de forma razonable sobre dicha vulneración y el estado de cualquier actividad de corrección y restauración por parte del Proveedor. A modo de ejemplo, la información solicitada de forma razonable puede incluir registros que demuestren el 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 en que sean relevantes para la vulneración o las actividades de corrección y restauración del Proveedor.

2.4 El Proveedor brindará a Kyndryl asistencia razonable para cumplir con cualquier obligación legal (incluidas las obligaciones de avisar a los reguladores o Interesados) de Kyndryl, los afiliados de Kyndryl y los Clientes (y sus clientes y afiliados) en relación con una Vulneración de seguridad.

2.5 El Proveedor no informará ni avisará a ningún tercero que una Vulneración de seguridad está relacionada directa o indirectamente con Kyndryl con o los Materiales de Kyndryl, a menos que Kyndryl lo apruebe por escrito o cuando así lo exija la ley. El Proveedor notificará a Kyndryl por escrito antes de distribuir cualquier notificación legalmente requerida a cualquier tercero, donde la notificación revele directa o indirectamente la identidad de Kyndryl.

2.6 En caso de una Vulneración de seguridad derivada del incumplimiento por parte del Proveedor de cualquier obligación en virtud de estos Términos:

(a) el Proveedor se hará cargo de los costes en los que incurra, así como de los costes reales en los que Kyndryl incurra, al proporcionar la notificación de la Vulneración de seguridad a los reguladores aplicables, otros organismos del gobierno y agencias reguladoras del sector pertinentes, los medios de comunicación (si así lo exige la legislación aplicable), Interesados, Clientes y otros,

(b) si Kyndryl lo solicita, el Proveedor establecerá y mantendrá a cargo del Proveedor un centro de atención para responder a las preguntas de los Interesados sobre la Vulneración de seguridad y sus consecuencias, durante 1 año después de la fecha en que se notificó la Vulneración de seguridad a dichos Interesados, o según lo requiera cualquier ley de protección de datos vigente, lo que brinde mayor protección. Kyndryl y el Proveedor trabajarán juntos para crear los guiones y otros materiales que utilizará el personal del centro de atención telefónica al responder a las consultas. Alternativamente, mediante notificación por escrito al Proveedor, Kyndryl puede establecer y mantener su propio centro de atención telefónica, en lugar de que el Proveedor establezca un centro de atención telefónica, y el Proveedor reembolsará a Kyndryl los costes reales en los que Kyndryl incurra para establecer y mantener dicho centro de atención telefónica, y

(c) el Proveedor reembolsará a Kyndryl los costes reales en los que incurra Kyndryl al brindar servicios de supervisión y restauración del crédito durante 1 año después de la fecha en que las personas afectadas por la vulneración que decidieron suscribirse a dichos servicios fueron notificadas de la Vulneración de seguridad, o según lo requiera cualquier ley de protección de datos vigente, lo que otorgue mayor protección.

3. Seguridad física y control de entrada (como se usa a continuación, «Instalaciones» significa una ubicación física donde el Proveedor aloja, trata o accede de otro modo a los Materiales de Kyndryl).

3.1 El Proveedor mantendrá controles de entrada físicos apropiados, como barreras, puntos de entrada controlados por tarjeta, cámaras de vigilancia y mostradores de recepción atendidos, para proteger contra la entrada no autorizada a las Instalaciones.

3.2 El Proveedor requerirá la aprobación autorizada para acceder a las instalaciones y áreas controladas dentro de las instalaciones, incluido cualquier acceso temporal, y limitará el acceso según las funciones del puesto de trabajo y la necesidad de negocio. Si el Proveedor otorga acceso temporal, su empleado autorizado acompañará a cualquier visitante mientras se encuentre en las Instalaciones y en cualquier área controlada.

3.3 El Proveedor implementará controles de acceso físico, incluidos controles de acceso de múltiples factores que sean coherente con las Mejores prácticas del sector, para restringir adecuadamente la entrada a áreas controladas dentro de las Instalaciones, registrará todos los intentos de entrada y conservará dichos registro durante al menos un año.

3.4 El Proveedor revocará el acceso a las Instalaciones y áreas controladas dentro de las Instalaciones cuando (a) termine la relación laboral de un empleado autorizado del Proveedor o (b) el empleado autorizado del Proveedor ya no tenga una necesidad de negocio válida para acceder. El Proveedor seguirá los procedimientos formales documentados de terminación de la relación laboral que incluyen una rápida eliminación de las listas de control de acceso y entrega de las tarjetas de acceso físico.

3.5 El Proveedor tomará precauciones para proteger toda la infraestructura física utilizada para respaldar los Servicios y Productos y el Manejo de la Tecnología de Kyndryl contra amenazas ambientales, tanto naturales

como provocadas por el hombre, tales como temperatura ambiente excesiva, incendio, inundación, humedad, robo y vandalismo.

4. Control de acceso, intervención, transferencia y separación

4.1 El Proveedor mantendrá una arquitectura documentada de seguridad de las redes que administra en su operación de los Servicios, su suministro de Productos y su Manejo de la Tecnología de Kyndryl. El Proveedor revisará por separado dicha arquitectura de redes y empleará medidas para impedir conexiones de red no autorizadas a los sistemas, aplicaciones y dispositivos de red, para garantizar la conformidad con los estándares de segmentación segura, aislamiento y defensa en profundidad. El Proveedor no utilizará tecnología inalámbrica para alojar y operar cualquier Servicio alojado; por lo demás, el Proveedor puede usar tecnología de red inalámbrica en su provisión de Servicios y Productos y en su Manejo de la Tecnología de Kyndryl, pero el Proveedor cifrará y requerirá una autenticación segura para dichas redes inalámbricas.

4.2 El Proveedor mantendrá medidas diseñadas para separar lógicamente e impedir la exposición o el acceso a los Materiales de Kyndryl por parte de personas no autorizadas. Además, el Proveedor mantendrá el aislamiento apropiado de su entorno de producción, no producción u otros y, si los Materiales de Kyndryl ya están presentes o se han transferido a un entorno de no producción (por ejemplo, para reproducir un error), entonces 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.

4.3 El Proveedor cifrará los Materiales de Kyndryl en tránsito y en reposo (a menos que el Proveedor demuestre a satisfacción razonable de Kyndryl que cifrar los Materiales de Kyndryl en reposo no es técnicamente viable). El Proveedor también cifrará todo soporte físico, si lo hubiera, como los soportes que contengan archivos de seguridad. El Proveedor mantendrá procedimientos documentados para la generación, emisión, distribución, almacenamiento, rotación, revocación, recuperación, copia de seguridad, destrucción, acceso y uso seguros de claves asociadas al cifrado de datos. El Proveedor garantizará que los métodos criptográficos específicos utilizados para dicho cifrado se ajusten a las Mejores prácticas del sector (como NIST SP 800-131a).

4.4 Si el Proveedor requiere acceder a los Materiales de Kyndryl, restringirá y limitará dicho acceso al nivel mínimo necesario para prestar y respaldar los Servicios y Productos. El Proveedor exigirá que dicho acceso, incluido el acceso administrativo a cualquier componente subyacente (es decir, el acceso privilegiado), sea individual, basado en funciones y sujeto a aprobación y validación regulares por parte de empleados autorizados siguiendo los principios segregación de funciones. El Proveedor mantendrá medidas para identificar y eliminar cuentas redundantes e inactivas. El Proveedor también revocará las cuentas con acceso privilegiado en un plazo de veinticuatro (24) horas después de finalizar la relación laboral del titular de la cuenta o de la solicitud de Kyndryl o de cualquier empleado autorizado del Proveedor, como el gestor del titular de la cuenta.

4.5 De acuerdo con las Mejores prácticas del sector, el Proveedor mantendrá medidas técnicas para aplicar la desconexión de sesiones inactivas tras exceder el tiempo de espera, el bloqueo de cuentas después de múltiples intentos erróneos de iniciar sesión, autenticación sólida de contraseñas y claves, así como medidas que exijan la modificación y almacenamiento seguros de dichas contraseñas y claves. Además, el Proveedor utilizará autenticación de multifactores para todos los accesos privilegiados que no se realicen mediante consola a cualquier Material de Kyndryl.

4.6 El Proveedor supervisará el uso del acceso privilegiado y mantendrá medidas de seguridad de la información y de gestión de sucesos diseñadas para: (a) identificar cualquier actividad y acceso sin autorización, (b) facilitar una respuesta oportuna y adecuada a dichas actividades y accesos, y (c) habilitar las auditorías del Proveedor, Kyndryl (de conformidad con sus derechos de verificación en estos Términos y sus derechos de auditoría en el Documento de transacción, en el acuerdo base asociado o en otro acuerdo relacionado entre las partes) y otros de conformidad con la política documentada del Proveedor.

4.7 El Proveedor conservará registros en los que almacene, de conformidad con las Mejores prácticas del sector, todos los accesos o actividades administrativos, de usuario u otros relacionados con los sistemas utilizados para proporcionar Servicios o Productos y Manejar la Tecnología de Kyndryl (y proporcionará esos registros a Kyndryl a petición). El Proveedor mantendrá medidas diseñadas para proteger contra el acceso sin autorización, modificación y destrucción accidental o deliberada de dichos registros.

4.8 El Proveedor aplicará protecciones informáticas para los sistemas que posee o gestiona, incluidos los sistemas de los usuarios finales, y que utiliza para proporcionar Servicios o Productos o Manejar la Tecnología de Kyndryl, y dichas protecciones incluirán: cortafuegos de punto final, cifrado de disco completo, tecnologías de detección y respuesta de terminales basadas en firma y sin firma para abordar las amenazas persistente avanzadas y de malware, bloqueos de pantalla basados en tiempo y soluciones de gestión de puntos finales que impongan los requisitos configuración de seguridad y aplicación de parches. Además, el Proveedor implementará controles técnicos y operativos que garanticen que solo se permita a los sistemas de usuarios finales conocidos y de confianza utilizar las redes del Proveedor.

4.9 De acuerdo con las Mejores prácticas del sector, el Proveedor mantendrá protecciones para los entornos del centro de datos donde se almacene o procese el Material de Kyndryl. Dichas protecciones incluyen tanto detección y prevención de intrusiones como contramedidas y mitigación de los ataques de denegación de servicio.

5. Integridad de los servicios y sistemas y control de la disponibilidad

5.1 El Proveedor: (a) realizará evaluaciones del riesgo de seguridad y privacidad al menos una vez al año, (b) realizará pruebas de seguridad y evaluará vulnerabilidades, incluido el escaneo automatizado de la seguridad del sistema y las aplicaciones y la piratería ética manual, antes del lanzamiento en producción y anualmente a partir de entonces, según corresponda a los Servicios y Productos con respecto a su Manejo de la Tecnología de Kyndryl, (c) reclutará a un tercero independiente cualificado para realizar pruebas de penetración coherentes con las Mejores prácticas del sector al menos una vez al año, con pruebas tanto automatizadas como manuales, (d) gestionará automáticamente y verificará periódicamente la conformidad con los requisitos de configuración de seguridad para cada componente de los Servicios y Productos y con respecto a su Manejo de la Tecnología de Kyndryl, y (e) corregirá las vulnerabilidades o incumplimientos identificados con sus requisitos de configuración de la seguridad en función del riesgo, capacidad de explotación e impacto asociados. El Proveedor tomará las medidas razonables para evitar la interrupción de los Servicios al realizar sus pruebas, evaluaciones, escaneos y ejecución de actividades correctivas. A petición de Kyndryl, el Proveedor proporcionará a Kyndryl un resumen por escrito de las actividades de pruebas de penetración más recientes del Proveedor, informe que incluirá como mínimo el nombre de las ofertas cubiertas por las pruebas, el número de sistemas o aplicaciones incluidos en las pruebas, las fechas de las pruebas, la metodología utilizada en las pruebas y un resumen de alto nivel de los resultados.

5.2 El Proveedor mantendrá políticas y procedimientos diseñados para administrar los riesgos asociados con la aplicación de cambios en los Servicios o Productos o con el Manejo de la Tecnología 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 razón del cambio, (b) los detalles y el plazo de implementación, (c) una declaración de riesgo que aborde el impacto sobre los Servicios y Productos, clientes de los Servicios o Materiales de Kyndryl, (d) el resultado esperado, (e) el plan de reversión, y (f) la aprobación por parte de los empleados autorizados del Proveedor.

5.3 El Proveedor mantendrá un inventario de todos los activos de TI que utilice para operar los Servicios, proporcionar Productos y Manejar la Tecnología de Kyndryl. El Proveedor supervisará y gestionará continuamente el estado (incluida la capacidad) y la disponibilidad de dichos activos de TI, Servicios, Productos y Tecnología de Kyndryl, incluidos los componentes subyacentes de dichos activos, Servicios, Productos y Tecnología de Kyndryl.

5.4 El Proveedor desplegará todos los sistemas que utilice en el desarrollo u operación de Servicios y Productos y en su Manejo de la Tecnología de Kyndryl a partir de imágenes de seguridad del sistema predefinidas o líneas de referencia de seguridad, que cumplan las Mejores prácticas del sector, como los puntos de referencia del Centro para la Seguridad de Internet (CIS).

5.5 Sin limitar las obligaciones del Proveedor ni los derechos de Kyndryl en virtud del Documento de transacción o del acuerdo base asociado entre las partes con respecto a la continuidad del negocio, el Proveedor evaluará por separado cada Servicio y Producto y cada sistema de TI utilizado en el Manejo de la Tecnología de Kyndryl en términos de los requisitos de continuidad de TI y del negocio y de recuperación tras desastres de acuerdo con las directrices de gestión de riesgos documentadas. El Proveedor se asegurará de que cada Servicio, Producto y Sistema de TI tenga, en la medida en que lo justifique dicha evaluación de riesgos, planes de

continuidad y recuperación tras desastres definidos, documentados, mantenidos y validados anualmente por separado de acuerdo con las Mejores prácticas del sector. El Proveedor se asegurará de que dichos planes estén diseñados para cumplir los tiempos de recuperación específicos que se definen en la Sección 5.6 a continuación.

5.6 Los objetivos de punto de recuperación específico («**RPO**») y los objetivos de tiempo de recuperación («**RTO**») con respecto a cualquier Servicio alojado son: RPO de 24 horas y RTO de 24 horas; sin embargo, el Proveedor cumplirá con cualquier RPO o RTO de menor duración que Kyndryl haya confirmado a un Cliente, inmediatamente después de que Kyndryl notifique al Proveedor por escrito de dicho RPO o RTO de menor duración (un correo electrónico constituye una notificación por escrito). En lo que respecta a todos los demás Servicios proporcionados por el Proveedor a Kyndryl, el Proveedor se asegurará de que sus planes de continuidad del negocio y recuperación tras desastres estén diseñados para cumplir RPO y RTO que permitan al Proveedor permanecer al corriente de todas sus obligaciones con Kyndryl en virtud del Documento de transacción y del acuerdo base asociado entre las partes, y estos Términos, incluidas sus obligaciones de proporcionar pruebas, soporte y mantenimiento de manera oportuna.

5.7 El Proveedor mantendrá medidas diseñadas para evaluar, probar y aplicar parches de advertencia de seguridad tanto a los Servicios y Productos como a los sistemas, redes, aplicaciones y componentes subyacentes asociados dentro del alcance de esos Servicios y Productos, así como los sistemas, redes, aplicaciones y los componentes subyacentes utilizados para Manejar la tecnología de Kyndryl. Una vez determinado que un parche de aviso de seguridad es aplicable y apropiado, el Proveedor implementará el parche de acuerdo con las directrices documentadas de gravedad y evaluación de riesgos. La implementación de los parches de advertencia de seguridad por parte del Proveedor estará sujeto a su política de gestión de cambios.

5.8 Si Kyndryl tiene motivos razonables para creer que el hardware o software que el Proveedor proporciona a Kyndryl puede contener elementos intrusivos, como spyware, malware o código malicioso, entonces el Proveedor cooperará oportunamente con Kyndryl para investigar y subsanar las inquietudes de Kyndryl.

6. Prestación de servicios

6.1 El Proveedor admitirá los métodos estándares del sector de autenticación federada para cualquier cuenta de usuarios o clientes de Kyndryl. El Proveedor aplicará las Mejores prácticas del sector para autenticar dichas cuentas de usuarios o clientes de Kyndryl (como el inicio de sesión único de multifactores administrado centralmente de Kyndryl, usando OpenID Connect o Security Assertion Markup Language).

7. Subcontratistas. Sin limitar las obligaciones del Proveedor ni los derechos de Kyndryl en virtud del Documento de transacción o del acuerdo base asociado entre las partes con respecto a la contratación de subcontratistas, el Proveedor se asegurará de que cualquier subcontratista que realice un trabajo para el Proveedor haya establecido controles de gobernanza para cumplir con los requisitos y las obligaciones que estos Términos imponen al Proveedor.

8. Soportes físicos. El Proveedor borrará de forma segura los soportes físicos destinados a la reutilización antes de dicha reutilización, y destruirá los soportes físicos que no estén destinados a la reutilización, de acuerdo con las Mejores prácticas del sector para el borrado de medios.

Artículo IX, Certificaciones e informes de servicios alojados

Este Artículo se aplica si el Proveedor proporciona un Servicio alojado a Kyndryl.

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

Certificaciones / Informes	**Plazo de tiempo**
Con respecto a los Servicios alojados del Proveedor: Certificación de conformidad con ISO 27001, Tecnología de la información, Técnicas de seguridad, Sistemas de gestión de seguridad de la información, y dicha certificación estará basada en la evaluación de un auditor independiente acreditado **O bien** SOC 2 Tipo 2: Un informe de un auditor independiente acreditado que demuestre su revisión de los sistemas, controles y operaciones del Proveedor de conformidad con un SOC 2 Tipo 2 (que incluya, como mínimo, seguridad, confidencialidad y disponibilidad)	El Proveedor obtendrá la certificación ISO 27001 en un plazo de 120 días a partir de la fecha de vigencia del Documento de transacción* o la Fecha de entrada en vigor** y después renovará la certificación basada en la evaluación de un auditor independiente acreditado cada 12 meses a partir de entonces (cada renovación se realizará según la versión más actual del estándar) El Proveedor obtendrá el informe SOC 2 Tipo 2 en un plazo de 240 días a partir de la fecha de vigencia del Documento de transacción* o Fecha de entrada en vigor**y después obtendrá un nuevo informe de un auditor independiente acreditado que demuestre su revisión de los sistemas, controles y operaciones del Proveedor de conformidad con un SOC 2 Tipo 2 (que incluya, como mínimo, seguridad, confidencialidad y disponibilidad) cada 12 meses a partir de ese momento * Si, a partir de dicha fecha de vigencia, el Proveedor brinda un Servicio alojado ** La fecha en que el Proveedor asume la obligación de prestar un Servicio alojado

1.2 Si el Proveedor lo solicita por escrito, y Kyndryl lo aprueba por escrito, el Proveedor podrá obtener una certificación o informe sustancialmente equivalentes a los mencionados anteriormente, entendiéndose que los plazos establecidos en la tabla anterior se aplicarían sin cambios con respecto a la certificación o informe sustancialmente equivalentes.

1.3 El Proveedor: (a) previa solicitud, proporcionará de inmediato a Kyndryl una copia de cada certificación e informe que el Proveedor está obligado a obtener y (b) resolverá sin demora cualquier deficiencia de control interno observada durante las revisiones SOC 2 o sustancialmente equivalente (si Kyndryl así lo aprueba).

Artículo X, Cooperación, verificación y corrección

Este Artículo se aplica si el Proveedor proporciona Servicios o Productos a Kyndryl.

1. Cooperación del Proveedor

1.1 Si Kyndryl tiene motivos para cuestionar si alguno de los Servicios o Productos puede haber contribuido, está contribuyendo 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.

1.2 Las partes acuerdan: (a) suministrar, previa solicitud, dicha información adicional, (b) ejecutar y suministrar mutuamente dichos documentos, y (c) realizar otro acto o cosa que la otra parte pueda solicitar razonablemente, con el fin de cumplir la intención de estos Términos y los documentos a los que se hace referencia en estos Términos. Por ejemplo, si Kyndryl lo solicita, el proveedor facilitará puntualmente los términos centrados en la privacidad y la seguridad de sus contratos escritos con Subencargados y subcontratistas, incluso, cuando el Proveedor tenga derecho a ello, permitiendo el acceso a los propios contratos.

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

2. Verificación (como se usa a continuación, «Instalaciones» significa una ubicación física donde el Proveedor aloja, trata o accede de otro modo a los Materiales de Kyndryl)

2.1 El Proveedor mantendrá un registro auditable que demuestre la conformidad con estos Términos.

2.2 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 Trate los 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.

2.3 Una verificación no se producirá más de una vez en cualquier período de 12 meses, a menos que: (a) Kyndryl esté validando la corrección del Proveedor de inquietudes derivadas de una verificación anterior durante el período de 12 meses o (b) se haya producido una Vulneración de seguridad y Kyndryl desee verificar la conformidad con las obligaciones pertinentes a la vulneración. En cualquier caso, Kyndryl proporcionará el mismo aviso por escrito con 30 días de anticipación que se ha especificado en la Sección 2.2 anterior, pero la urgencia de abordar una Vulneración de seguridad puede requerir que Kyndryl realice una verificación con un aviso por escrito de menos de 30 días.

2.4. Un regulador u otro Responsable puede ejercer los mismos derechos que Kyndryl en las Secciones 2.2 y 2.3, entendiendo que un regulador puede ejercer cualquier derecho adicional que tenga en virtud de la ley.

2.5 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.

3. Programa antifalsificación

3.1 Si los Productos 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 falsificaciones para, ante todo, evitar que el Proveedor suministre componentes falsificados a Kyndryl y, en segundo lugar, detectar y subsanar cualquier caso en el que el Proveedor suministre por error componentes falsificados a Kyndryl. El Proveedor impondrá esta misma obligación de mantener y seguir un programa documentado de prevención de falsificaciones a todos sus proveedores que suministren componentes electrónicos que estén incluidos en los Productos del Proveedor a Kyndryl.

4. Corrección

4.1 Si el Proveedor incumple cualquiera de sus obligaciones en virtud de estos Términos, y ese error provoca una Vulneración de seguridad, entonces el Proveedor corregirá el error y remediará los efectos dañinos de la Vulneración de seguridad, realizando dichas actividades correctivas según las indicaciones y plazos razonables de Kyndryl. Sin embargo, si la Vulneración de seguridad se deriva de la prestación por parte del Proveedor de un Servicio alojado multiarrendatario y, en consecuencia, afecta a muchos clientes del Proveedor, incluido Kyndryl, el Proveedor, dada la naturaleza de la Vulneración de seguridad, corregirá oportuna y adecuadamente el error y remediará los efectos nocivos de la Vulneración de Seguridad, teniendo debidamente en cuenta cualquier indicación de Kyndryl sobre dichas actividades de corrección y remediación. Sin perjuicio de lo anterior, el Proveedor deberá avisar a Kyndryl sin dilación indebida si el Proveedor ya no puede cumplir con las obligaciones establecidas por la ley de protección de datos vigente.

4.2 Kyndryl tendrá derecho a participar en la subsanación de cualquier Vulneración de seguridad a la que se hace referencia en la Sección 4.1, según considere apropiado o necesario, y el Proveedor será responsable de sus costes y gastos para corregir su actuación y de los costes y gastos de subsanación en los que incurran las partes con respecto a cualquier Vulneración de seguridad.

4.3 Por ejemplo, los costes y gastos de corrección asociados con una Vulneración de seguridad podrían incluir aquellos para detectar e investigar una Vulneración de seguridad, determinar las responsabilidades bajo las leyes y regulaciones aplicables, proporcionar notificaciones de vulneraciones, establecer y mantener centros de atención telefónica, proporcionar servicios de supervisión y restauración del crédito, volver a cargar datos, corregir defectos del producto (incluso a través del Código fuente u otro desarrollo), contratar a terceros para ayudar con lo anterior u otras actividades pertinentes, y otros costes y gastos que sean necesarios para subsanar los efectos dañinos de la Vulneración de seguridad. Para mayor claridad, los costes y gastos de corrección no incluirían la pérdida de ganancias, negocios, valor, ingresos, fondo de comercio ni ahorros anticipados de Kyndryl.