Seguridad de los Datos y Fundamentos de Privacidad de Kyndryl

1. Definiciones

Los términos en mayúscula utilizados en este documento tienen los significados que se dan a continuación o, si no se definen a continuación, los significados que se dan en el contrato por escrito aplicable entre Kyndryl y el Cliente para los Servicios de Kyndryl.

Cliente: entidad a la que Kyndryl proporciona los Servicios de Kyndryl bajo un Documento de Servicios de Kyndryl.

Componente: aplicación, plataforma o elementos de infraestructura de un Servicio de Kyndryl que Kyndryl opera y gestiona.

Contenido: incluye todos los datos, software e información que el Cliente o sus usuarios autorizados proporcionan, autorizan su acceso o introducen en los Servicios de Kyndryl.

DSP: este documento de Seguridad de los Datos y Fundamentos de Privacidad de Kyndryl.

Documento de Servicios de Kyndryl: Documento Transaccional y cualquier otro documento que se incorpore a un contrato por escrito entre Kyndryl y un Cliente, y que incluye los detalles de un Servicio de Kyndryl específico.

Servicios de Kyndryl: (a) ofertas de servicios de Kyndryl, incluidas las ofertas de servicios de aplicaciones o de infraestructura que Kyndryl presta y dedica o personaliza para un Cliente, y (b) cualquier otro servicio, incluidos consultoría, mantenimiento o soporte, que Kyndryl proporciona a un Cliente.

Incidente de Seguridad: acceso y uso no autorizado del Contenido.

Documento Transaccional: documento que describe los detalles de las transacciones, tales como los cargos, la descripción e información sobre un Servicio de Kyndryl. Algunos ejemplos de Documentos Transaccionales son: las especificaciones de trabajo, las descripciones de servicios, los documentos de pedido y las facturas de un Servicio de Kyndryl. Puede haber más de un Documento Transaccional aplicable a una transacción.

2. Visión general

Las medidas técnicas y organizativas proporcionadas en este DSP se aplican a los Servicios de Kyndryl (incluido cualquier Componente) solo cuando Kyndryl haya acordado expresamente cumplir con el DSP en un contrato por escrito entre Kyndryl y el Cliente. Para mayor claridad, esas medidas no se aplican cuando el Cliente es responsable de la seguridad y la privacidad, o cuando así se especifique en un Documento de Servicios de Kyndryl o a continuación.

a. El Cliente es responsable de determinar si un Servicio de Kyndryl se adecúa a sus necesidades de uso y de implementar y gestionar las medidas de seguridad y privacidad para los componentes no proporcionados ni gestionados por Kyndryl dentro de dicho servicio. Entre los ejemplos de responsabilidades del Cliente respecto a los Servicios de Kyndryl se incluyen: (1) la seguridad de los sistemas y las aplicaciones creados o implementados por el Cliente sobre un servicio de infraestructura como servicio o plataforma como servicio, o sobre infraestructura, Componentes o software que Kyndryl gestione para un Cliente, y (2) control de acceso de usuarios finales del Cliente y configuración de seguridad a nivel de aplicación para un servicio de software como servicio que Kyndryl gestione para un Cliente o uno de servicio de aplicación que Kyndryl preste a un Cliente.

b. El Cliente reconoce que Kyndryl puede modificar este DSP, cada cierto tiempo y a su sola discreción, y que tales modificaciones sustituirán a las versiones anteriores y tendrán efecto a partir de la fecha en que Kyndryl publique la versión modificada. Con independencia de cualquier disposición en contra en cualquier contrato por escrito entre Kyndryl y el Cliente, el propósito de cualquier modificación será: (1) mejorar o aclarar los compromisos existentes, (2) permitir a Kyndryl priorizar su enfoque de seguridad para resolver problemas y amenazas de ciberseguridad e información sobre datos cambiante, (3) alinearse con los estándares actuales y las leyes aplicables, o (4) proporcionar características técnicas y funcionalidades adicionales. Las modificaciones no degradarán las características técnicas o funcionalidades de seguridad o protección de datos de los Servicios de Kyndryl.

c. En caso de conflicto entre este DSP y un Documento de Servicios de Kyndryl, el Documento de Servicios de Kyndryl prevalecerá y, si los términos en conflicto se encuentran en un Documento

Transaccional, estos se identificarán como prevalentes sobre los términos de este DSP y solo serán de aplicación a la transacción específica.

3. Protección de Datos

a. Kyndryl tratará todo el Contenido como confidencial revelándolo sólo a sus empleados, contratistas y proveedores (incluidos los subencargados del tratamiento de datos), y sólo en la medida en que sea necesario para prestar los Servicios de Kyndryl.

b. Las medidas de seguridad y privacidad para cada Servicio de Kyndryl están diseñadas de acuerdo con las prácticas de seguridad y privacidad desde el diseño (by design) de Kyndryl, con el fin de proteger el Contenido tratado al prestar un Servicio de Kyndryl y mantener la disponibilidad de ese Contenido conforme al contrato suscrito por escrito entre Kyndryl y el Cliente, incluidos los Documentos de Servicios de Kyndryl aplicables.

c. La información adicional de seguridad y privacidad específica de un Servicio de Kyndryl puede estar disponible en el Documento de Servicios de Kyndryl correspondiente o en otra documentación estándar, todo ello para ayudar al Cliente en su evaluación inicial y continua sobre la idoneidad de un Servicio de Kyndryl para su uso por parte del Cliente. Dicha información puede incluir evidencia de certificaciones y acreditaciones obtenidas, información relacionada con dichas certificaciones y acreditaciones, fichas de datos, preguntas frecuentes y otra documentación disponible de manera general. Si se le solicita, Kyndryl facilitará al Cliente la documentación estándar disponible para cumplimentar los cuestionarios de seguridad o privacidad elegidos por el Cliente.

4. Políticas de Seguridad

a. Kyndryl mantendrá y seguirá las políticas y prácticas escritas de seguridad de IT que forman parte integral del negocio de Kyndryl y son de obligado cumplimiento para todos los empleados de Kyndryl. El Director de Seguridad de la Información de Kyndryl (CISO) mantendrá la responsabilidad y la supervisión ejecutiva sobre dichas políticas, incluyendo la gobernanza formal y la dirección sobre su revisión, la formación de los empleados y la ejecución del cumplimiento de normativas.

b. Kyndryl revisará sus políticas de seguridad de IT como mínimo una vez al año y realizará modificaciones de las mismas según estime razonable para mantener la protección de los Servicios de Kyndryl y su Contenido.

c. Kyndryl mantendrá y seguirá sus requisitos obligatorios de verificación de empleo para las nuevas contrataciones y hará que se apliquen tales requisitos a todas sus filiales en propiedad plena. De acuerdo con los procedimientos y procesos internos de Kyndryl, estos requisitos se revisarán periódicamente e incluirán, sin necesidad de limitarse a ello, comprobaciones de antecedentes penales, validación de la prueba de identidad y comprobaciones adicionales que Kyndryl estime necesarias. Cada empresa de Kyndryl es responsable de implementar estos requisitos en su contratación, según corresponda y lo permita la legislación local aplicable.

d. Los empleados de Kyndryl completarán anualmente una formación sobre seguridad y privacidad y certificarán cada año que van a cumplir con las políticas de conducta ética empresarial, confidencialidad y seguridad de Kyndryl, tal y como se establece en las Directrices de Conducta Empresarial de Kyndryl. Adicionalmente, se proporcionará formación complementaria a las personas con acceso privilegiado a Componentes, específica al papel que desempeñan en la operativa y el soporte de los Servicios de Kyndryl, todo ello según sea necesario para mantener la conformidad y las certificaciones obtenidas indicadas en cualquier Documento de Servicios de Kyndryl.

5. Cumplimiento

a. Kyndryl mantendrá la conformidad y la acreditación de los Servicios de Kyndryl tal como se define en el Documento de Servicios de Kyndryl.

b. Previa solicitud, Kyndryl proporcionará evidencias de la conformidad y de la acreditación requerida según el punto 5a., tales como certificados, testificaciones o informes que sean resultado de auditorías independientes acreditadas de terceros (que se efectuarán con la regularidad requerida por el estándar pertinente).

c. Kyndryl es responsable de estas medidas de privacidad y seguridad de los datos, incluso si Kyndryl utiliza un contratista o proveedor (incluidos los subencargados del tratamiento) para la prestación de o el soporte a un Servicio de Kyndryl.

6. Incidentes de Seguridad

a. Para la gestión de incidentes de seguridad informática, Kyndryl mantendrá y seguirá las políticas de respuesta a incidentes conforme a las directrices del NIST (National Institute of Standards and Technology) del Departamento de Comercio de los Estados Unidos, o los estándares sectoriales equivalentes, y cumplirá con los términos sobre notificación de violaciones de seguridad de datos contenidos en el contrato escrito aplicable entre Kyndryl y el Cliente.

b. Kyndryl investigará los Incidentes de Seguridad que detecte y, para el alcance de los Servicios de Kyndryl, definirá y ejecutará un plan de respuesta adecuado. El Cliente puede notificar a Kyndryl la sospecha de una vulnerabilidad o incidente enviando una solicitud a través del proceso de notificación específico al Servicio de Kyndryl (según se indique en un Documento de Servicios de Kyndryl) o, en ausencia de dicho proceso, mediante el envío de una solicitud de soporte técnico.

c. Kyndryl notificará al Cliente, sin incurrir en demoras indebidas, cualquier Incidente de Seguridad que le sea conocido o que Kyndryl sospeche de forma razonable que puede afectar al Cliente. Kyndryl suministrará al Cliente la información razonable que sea solicitada acerca del Incidente de Seguridad, así como el estado de las actividades de remediación y restauración llevadas a cabo por Kyndryl.

7. Seguridad Física y Control de Entrada

a. Kyndryl mantendrá los controles de entrada física adecuados, como barreras, puntos de entrada controlados con tarjeta de identidad, cámaras de vigilancia y recepcionistas, para impedir la entrada no autorizada a las instalaciones gestionadas por Kyndryl (centros de datos) que se utilicen para alojar los Servicios de Kyndryl. Los puntos de entrada auxiliares a estos centros de datos, como las áreas de entrega o los muelles de carga, se controlarán y aislarán de los recursos informáticos.

b. El acceso a los centros de datos gestionados de Kyndryl y a las áreas controladas en estos centros de datos estará limitado según el puesto de trabajo y estará sujeto a aprobación autorizada. Dicho acceso quedará registrado, y los registros se conservarán durante un período mínimo de al menos un (1) año. Kyndryl revocará el acceso a los centros de datos gestionados por Kyndryl en caso de terminarse la relación laboral con un empleado autorizado. Kyndryl llevará a cabo los procedimientos formales documentados 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.

c. Todas las personas a las que se dé permiso de acceso temporal a las instalaciones de un centro de datos gestionado por Kyndryl o a un área controlada de este centro de datos se registrarán a la entrada de las instalaciones, deben proporcionar una prueba de identidad durante el registro y deberán ir acompañados por personal autorizado. El acceso temporal, incluidas las entregas, se programará con antelación y requerirá aprobación por parte de personal autorizado.

d. Kyndryl tomará precauciones para proteger la infraestructura física de las instalaciones del centro de datos gestionadas por Kyndryl frente a amenazas medioambientales, tanto naturales como artificiales, como temperatura ambiental excesiva, incendios, inundaciones, humedad, robo y vandalismo.

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

a. Kyndryl revisará la arquitectura de seguridad de los Componentes, incluidas las 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 estándares de defensa en profundidad antes de su implementación.

b. Kyndryl puede utilizar tecnología de red inalámbrica en su mantenimiento y soporte de los Servicios de Kyndryl y los Componentes asociados. Estas redes inalámbricas, si las hubiera, estarán cifradas y requerirán autenticación segura.

c. En los Servicios de Kyndryl, ésta mantendrá medidas diseñadas para la separación lógica y para evitar que el Contenido quede expuesto a personas no autorizadas o que éstas accedan a dicho Contenido. Kyndryl mantendrá un aislamiento adecuado de sus entornos productivos y no productivos y, si el Contenido se transfiere a un entorno no productivo, por ejemplo, para reproducir un error a petición del Cliente, las protecciones de seguridad y privacidad en el entorno no productivo serán equivalentes a las del productivo.

d. Kyndryl cifrará el Contenido que no esté destinado a visionado público o sin autenticación cuando transfiera Contenido a través de redes públicas y habilitará el uso de un protocolo criptográfico, tales

como HTTPS, SFTP o FTPS, para la transferencia segura de Contenido por parte del Cliente a o desde los Servicios de Kyndryl a través de redes públicas.

e. Kyndryl cifrará el Contenido en reposo si así se especifica y en la forma que se especifique en un Documento de Servicios de Kyndryl. Si el Servicio de Kyndryl incluye la gestión de claves criptográficas, Kyndryl mantendrá los procedimientos documentados para la generación, emisión, distribución, almacenamiento, rotación, revocación, recuperación, copia de seguridad, destrucción, acceso y uso segura de claves.

f. Si Kyndryl necesita acceso al Contenido para prestar los Servicios de Kyndryl, y si este acceso lo gestiona Kyndryl, restringirá dicho acceso al nivel mínimo necesario. Este acceso, incluido el acceso administrativo a los Componentes subyacentes (acceso privilegiado), será individual, se basará en roles y estará sujeto a aprobación y validación regular por parte del personal de Kyndryl conforme a los principios de separación de funciones. Kyndryl mantendrá medidas para identificar y eliminar cuentas inactivas y redundantes con acceso privilegiado y revocará inmediatamente este acceso en el momento de terminar la relación laboral con el titular de la cuenta o cuando lo solicite personal de Kyndryl autorizado como, por ejemplo, el director del titular de la cuenta.

g. De manera coherente con las prácticas estándar del sector, y en la medida en que sean soportadas se admita de forma nativa en cada Componente, Kyndryl mantendrá medidas técnicas que impongan tiempo de expiración en sesiones inactivas, bloqueo de cuentas tras diversos intentos fallidos de inicio de sesión, autenticación con contraseña o frase de contraseña fuertes, así como medidas que requieran la transferencia y el almacenamiento seguros de estas contraseñas y frases de contraseñas.

h. Kyndryl supervisará el uso de acceso privilegiado y mantendrá la información de seguridad y las medidas de gestión de eventos diseñadas para: (1) identificar la actividad y el acceso no autorizados, (2) facilitar una respuesta adecuada y oportuna, y (3) habilitar las auditorías internas y externas independientes de acuerdo con la política documentada de Kyndryl.

i. Los registros en los que se registren acceso y actividad privilegiados se conservarán en conformidad con la política de Kyndryl. Kyndryl mantendrá medidas diseñadas para la protección en caso de acceso no autorizado, modificación y destrucción accidental o deliberada de estos registros.

j. En la medida en que esté soportada por la funcionalidad del sistema operativo o del dispositivo nativo, Kyndryl mantendrá protecciones informáticas para los sistemas de usuario final que incluyen, aunque no necesariamente se limitan a, cortafuegos de puntos finales (endpoint firewalls), cifrado completo de disco, detección de malware y su eliminación, bloqueos de pantalla basados en tiempo y soluciones de gestión de puntos finales (endpoint) que impongan tanto los requerimientos configuración de seguridad como de parcheado (patching).

k. Kyndryl saneará de forma segura los soportes físicos que tenga intención de reutilizar antes de su reutilización y destruirá los soportes físicos que no pretenda reutilizar, de forma coherente con las directrices NIST para el saneamiento de soportes.

9. Control de Disponibilidad e Integridad del Servicio

a. Kyndryl: (1) realizará evaluaciones de riesgos de seguridad y privacidad de los Servicios de Kyndryl al menos una vez al año, (2) llevará a cabo pruebas de seguridad y evaluaciones de vulnerabilidad de los Servicios de Kyndryl antes del lanzamiento en producción y anualmente a partir del mismo, (3) realizará pruebas de intrusión en capacidades y servicios antes del lanzamiento en producción y anualmente a partir del mismo, (4) efectuará escaneos de vulnerabilidades automatizados de Componentes subyacentes de los Servicios de Kyndryl siguiendo las mejores prácticas de configuración de seguridad del sector, (5) resolverá las vulnerabilidades identificadas en las pruebas de seguridad y el análisis, en función del riesgo asociado, su explotabilidad e impacto, y (6) dará los pasos razonables para evitar la interrupción de los Servicios de Kyndryl al realizar sus pruebas, evaluaciones, escaneos y ejecución de actividades de reparación.

b. Kyndryl mantendrá medidas diseñadas para evaluar, probar y aplicar parches de advertencia de seguridad a los Servicios de Kyndryl y sus sistemas, redes, aplicaciones y componentes subyacentes asociados que estén dentro del alcance de dichos Servicios de Kyndryl. Tras determinar que un parche de advertencia de seguridad es aplicable y adecuado, Kyndryl implementará dicho parche conforme con las directrices documentadas de evaluación del riesgo y la severidad, según la clasificación de parches Common Vulnerability Scoring System, si está disponible. La

implementación de parches de advertencia de seguridad estará sujeta a la política de gestión de cambios de Kyndryl.

c. Kyndryl mantendrá políticas y procedimientos diseñados para gestionar los riesgos asociados con los cambios realizados en los Servicios de Kyndryl. Con anterioridad a su implementación, las modificaciones hechas a un Servicio de Kyndryl, incluidos los sistemas, las redes y los Componentes subyacentes, se documentarán en una solicitud de cambio registrada que incluya una descripción y el motivo del cambio, los detalles y la programación de la implementación, una declaración de riesgos enfocada en el impacto en el Servicio de Kyndryl y sus clientes, el resultado esperado, el plan de reversión y la aprobación documentada del personal autorizado para acordar el cambio.

d. Kyndryl mantendrá un inventario de todos los activos de tecnología de la información utilizados en la operativa de los Servicios de Kyndryl. Kyndryl monitorizará y gestionará continuamente el estado, incluida la capacidad, y la disponibilidad de los Servicios de Kyndryl y los Componentes subyacentes.

e. Cada Servicio de Kyndryl se evaluará por separado para determinar los requisitos de continuidad del negocio y de recuperación ante desastres mediante un análisis de impacto en el negocio y evaluaciones de riesgos adecuados para identificar y priorizar las funciones críticas del negocio. En la medida en que se garantice en dichas evaluaciones de riesgos, cada Servicio de Kyndryl dispondrá de planes separados de recuperación ante desastres y continuidad del negocio definidos, documentados, mantenidos y validados anualmente, coherentes con las prácticas estándares del sector. Los objetivos de tiempo y punto de recuperación para un Servicio de Kyndryl, si se proporcionan en el Documento de Servicios de Kyndryl correspondiente, se establecerán tomando en consideración la arquitectura y el uso previsto del Servicio de Kyndryl. Los soportes físicos destinados al almacenamiento externo, si los hubiera, tales como los que contienen archivos de copia de seguridad, se cifrarán antes de su transporte.