Segurança de Dados e Princípios de Privacidade da Kyndryl

1. Definições

Os termos com iniciais maiúsculas usados neste documento têm os significados fornecidos abaixo ou, caso não estejam definidos abaixo, os significados fornecidos no contrato por escrito aplicável entre a Kyndryl e o Cliente para os Serviços Kyndryl.

Cliente – é a entidade à qual a Kyndryl está fornecendo os Serviços Kyndryl que fazem parte de um Documento de Serviços Kyndryl.

Componentes – são o aplicativo, a plataforma ou os elementos da infraestrutura de um Serviço Kyndryl que é operado e gerenciado pela Kyndryl.

Conteúdo – consiste em todos os dados, software e informações que o Cliente ou seus usuários autorizados fornecem, autorizam o acesso ou inserem nos Serviços Kyndryl.

DSP – trata-se desde documento Segurança de Dados e Princípios de Privacidade da Kyndryl.

Documento de Serviços Kyndryl – é um Documento de Transação e todo documento incorporado em um contrato por escrito entre a Kyndryl e o Cliente, cuja finalidade seja especificar os detalhes de um determinado Serviço Kyndryl.

Serviços Kyndryl – são as ofertas de serviços Kyndryl, incluindo ofertas de serviços de infraestrutura ou de aplicativo fornecidas pela Kyndryl e customizadas ou desenvolvidas para um Cliente e quaisquer outros serviços fornecidos pela Kyndryl a um Cliente, incluindo consultoria, manutenção ou suporte.

Incidente de Segurança – definido como um acesso não autorizado e uso não autorizado de Conteúdo.

Documento de Transação – é um documento que detalha as particularidades das transações, como encargos e suas descrições, além de informações sobre um Serviço Kyndryl. Os exemplos de Documentos de Transação incluem declarações de trabalho, descrições de serviços, documentos de pedidos e faturas referentes a um Serviço Kyndryl. Pode haver mais de um Documento de Transação aplicável a uma transação.

2. Visão Geral

As medidas técnicas e organizacionais fornecidas neste DSP aplicam-se somente aos Serviços Kyndryl (incluindo Componentes) em relação aos quais a Kyndryl concordou expressamente com o cumprimento do DSP, por meio de um contrato por escrito estabelecido entre a Kyndryl e o Cliente. Para maior clareza, essas medidas não se aplicarão quando o Cliente for responsável pelas questões de segurança e privacidade, ou conforme especificado abaixo ou em um Documento de Serviços Kyndryl.

a. O Cliente é responsável por determinar se um Serviço Kyndryl é adequado para seu próprio uso e por implementar e gerenciar as medidas de segurança e privacidade para os componentes que não são fornecidos ou gerenciados pela Kyndryl dentro desses Serviços Kyndryl. Os exemplos de responsabilidades do Cliente em relação aos Serviços Kyndryl incluem: (1) a segurança de sistemas e aplicativos desenvolvidos ou implementados pelo Cliente sobre uma oferta de infraestrutura como serviço ou de plataforma como serviço ou com base em uma infraestrutura, Componentes ou software que a Kyndryl gerencia para o Cliente e (2) a configuração de segurança do Cliente no nível do aplicativo e o controle de acesso do usuário final para uma oferta de software como serviço que a Kyndryl gerencia para um Cliente ou uma oferta de serviço de aplicativo fornecida pela Kyndryl para um Cliente.

b. O Cliente reconhece que a Kyndryl pode modificar este DSP regularmente, a critério exclusivo da Kyndryl, e que tais modificações substituirão as versões anteriores assim que a versão modificada for publicada pela Kyndryl. Sem prejuízo do disposto, qualquer modificação contrária a qualquer contrato firmado entre a Kyndryl e o Cliente tem como objetivo: (1) melhorar ou esclarecer os compromissos existentes, (2) permitir que a Kyndryl priorize corretamente seu foco em segurança, tomando medidas adequadas para situações nas quais há aumento de dados e ameaças e problemas de segurança cibernética, (3) manter o alinhamento com padrões atualmente adotados e com as leis aplicáveis, ou (4) fornecer recursos e funcionalidades adicionais. Tais modificações não comprometerão os recursos de segurança ou de proteção de dados ou a funcionalidade dos Serviços Kyndryl.

c. Se houver conflito entre este DSP e um Documento de Serviços Kyndryl, o Documento de Serviços Kyndryl prevalecerá e, caso façam parte de um Documento de Transação, os termos conflitantes

serão identificados como substitutos dos termos deste DSP e se aplicarão apenas à transação específica.

3. Proteção de Dados

a. A Kyndryl tratará como confidencial todo Conteúdo, não divulgando-o a terceiros, com exceção de funcionários, contratados e fornecedores (incluindo subprocessadores) da Kyndryl e somente na medida necessária para o fornecimento dos Serviços Kyndryl.

b. As medidas de segurança e privacidade para cada Serviço Kyndryl são implementadas de acordo com as práticas de segurança e privacidade da Kyndryl, desenvolvidas para proteger o Conteúdo processado por um Serviço Kyndryl, e para manter a disponibilidade de tal Conteúdo de acordo com o disposto no contrato por escrito firmado entre a Kyndryl e o Cliente, incluindo os Documentos de Serviços Kyndryl aplicáveis.

c. Informações adicionais de segurança e privacidade específicas para um Serviço Kyndryl podem ser disponibilizadas no Documento de Serviços Kyndryl relevante ou em outra documentação padrão, com o objetivo de ajudar na avaliação inicial e contínua a respeito da compatibilidade de um Serviço Kyndryl com as necessidades de uso do Cliente. Tais informações podem incluir a evidência de certificações estabelecidas, informações relacionadas a tais certificações, planilhas de dados, FAQs e outra documentação disponível de forma geral. A Kyndryl direcionará o Cliente para a documentação padrão disponível, caso solicitada a preencher questionários sobre segurança ou privacidade escolhidos pelo Cliente.

4. Políticas de Segurança

a. A Kyndryl manterá e seguirá as práticas e políticas de segurança de TI estabelecidas por escrito e que são inerentes aos negócios da Kyndryl e obrigatórias para todos os funcionários da Kyndryl. O Diretor Executivo de Segurança da Informação da Kyndryl é responsável pela aplicação e supervisão executiva dessas políticas, incluindo o gerenciamento formal de ações de controle e revisão, treinamento de funcionários e o cumprimento das políticas de conformidade.

b. A Kyndryl revisará suas políticas de segurança de TI pelo menos uma vez por ano e fará as correções que considerar cabíveis para manter a proteção dos Serviços e do Conteúdo da Kyndryl.

c. A Kyndryl manterá e seguirá seus requisitos obrigatórios padrão de verificação de funcionários para todas as novas contratações, estendendo tais requisitos para as subsidiárias pertencentes integralmente à Kyndryl. De acordo com os processos e procedimentos internos da Kyndryl, esses requisitos serão revisados periodicamente e incluem, mas não se limitam a, verificações de antecedentes criminais, validação de comprovante de identidade e verificações adicionais, conforme a Kyndryl julgar necessário. Cada empresa Kyndryl é responsável por implementar esses requisitos em seu processo de contratação conforme aplicável e permitido pela legislação local.

d. Os funcionários Kyndryl concluirão o treinamento em segurança e privacidade anualmente fornecido pela Kyndryl e certificarão cada ano que irão obedecer às políticas de conduta comercial ética, confidencialidade e segurança da Kyndryl, conforme estabelecido nas Diretrizes de Conduta Comercial da Kyndryl. Treinamentos adicionais serão fornecidos para pessoas que receberem acesso privilegiado a Componentes específicos para sua função, no contexto de operação e suporte aos Serviços Kyndryl e conforme necessário para a manutenção da conformidade e dos credenciamentos indicados nos Documentos de Serviços Kyndryl relevantes.

5. Conformidade

a. A Kyndryl manterá a conformidade e a certificação dos Serviços Kyndryl, conforme definidos em um Documento de Serviços Kyndryl.

b. Mediante solicitação, a Kyndryl fornecerá as evidências de conformidade e credenciamento exigidas pelo item 5a., tais como certificados, atestados ou relatórios resultantes de auditorias certificadas de terceiros independentes (tais auditorias ocorrerão com a frequência exigida pelo padrão relevante).

c. A Kyndryl é responsável por tais medidas de privacidade e segurança de dados, mesmo que utilize empresas contratadas ou fornecedores (incluindo subprocessadores) para o fornecimento ou o suporte de um Serviço Kyndryl.

6. Incidentes de Segurança

a. A Kyndryl manterá e seguirá as políticas de resposta a incidentes documentadas, de acordo com as diretrizes do NIST (National Institute of Standards and Technology), Departamento de Comércio dos Estados Unidos, ou os padrões de mercado equivalentes, para o tratamento de incidentes de segurança de computadores, estando de acordo com os termos de notificação de violação de dados do contrato por escrito aplicável estabelecido entre a Kyndryl e o Cliente.

b. A Kyndryl investigará os Incidentes de Segurança dos quais tomar conhecimento e, dentro do escopo dos Serviços Kyndryl, definirá e executará um plano de resposta adequado. O Cliente poderá notificar a Kyndryl a respeito de uma vulnerabilidade ou de um incidente suspeitos, enviando uma solicitação por meio do processo de relatório de incidentes específico para o Serviço Kyndryl (conforme citado em um Documento de Serviços Kyndryl) ou, na ausência de tal processo, enviando uma solicitação de suporte técnico.

c. A Kyndryl notificará imediatamente o Cliente quando da confirmação de um Incidente de Segurança conhecido ou que muito provavelmente afetará o Cliente. A Kyndryl fornecerá ao Cliente as informações solicitadas corretas sobre tal Incidente de Segurança, além do status de quaisquer atividades de correção e restauração executadas pela Kyndryl.

7. Controle de Segurança e Entrada Física

a. A Kyndryl manterá controles adequados de entrada física, como barreiras, pontos de entrada controlados por cartão, câmeras de vigilância e recepção com funcionários para oferecer proteção contra a entrada não autorizada nas instalações gerenciadas pela Kyndryl (Centros de Dados), usadas para a hospedagem de Serviços Kyndryl. Os pontos de entrada adicionais existentes nesses Centros de Dados, tais como áreas de distribuição e docas de carga, serão controlados e isolados dos recursos de computação.

b. O acesso aos Centros de Dados gerenciados pela Kyndryl e às áreas controladas dentro desses Centros de Dados será limitado de acordo com o cargo e está sujeito à aprovação autorizada. Tais acessos serão registrados e esses registros serão mantidos por no mínimo um ano. Mediante o desligamento de um funcionário autorizado, a Kyndryl revogará o acesso deste aos Centros de Dados por ela gerenciados. A Kyndryl seguirá os procedimentos formais de desligamento documentados que incluem a remoção imediata das listas de controle de acesso e a devolução de crachás de acesso físico.

c. Qualquer pessoa que receba permissão temporária para entrar nas instalações de um Centro de Dados gerenciado pela Kyndryl ou em uma área controlada dentro de um Centro de Dados, deve fornecer um comprovante de identidade no momento do registro e será acompanhada por pessoal autorizado. Qualquer autorização temporária para entrar, incluindo entregas, será agendada com antecedência e exigirá aprovação da equipe autorizada.

d. A Kyndryl tomará todas as precauções para proteger a infraestrutura física das instalações de um Centro de Dados por ela gerenciado contra ameaças ambientais, tanto naturais quanto artificiais, como temperatura ambiente excessiva, incêndios, inundações, umidade, roubos e vandalismo.

8. Controle de Acesso, Intervenção, Transferência e Desligamento

a. Antes da implementação, a Kyndryl revisará a arquitetura de segurança dos Componentes, incluindo medidas projetadas para evitar conexões de rede não autorizadas com sistemas, aplicativos e dispositivos de rede, seguindo a conformidade com seus padrões de segmentação segura, isolamento e defesa em profundidade.

b. A Kyndryl pode utilizar tecnologia de rede wireless na manutenção e no suporte de Serviços Kyndryl e dos Componentes associados. Tais redes wireless, se houver, serão criptografadas e exigirão autenticação segura.

c. A Kyndryl manterá medidas para um Serviço Kyndryl que são projetadas para separar logicamente e evitar que o Conteúdo seja exposto a ou acessado por pessoas não autorizadas. A Kyndryl manterá o isolamento adequado de seus ambientes de produção e não produção e, caso o Conteúdo seja transferido para um ambiente de não produção, por exemplo, para reproduzir um erro, mediante solicitação do Cliente, as medidas de segurança e proteção de privacidade em tal ambiente serão equivalentes às aplicadas no ambiente de produção.

d. A Kyndryl criptografará o Conteúdo não destinado à visualização pública ou não autenticada ao usar redes públicas para a transferência de Conteúdo e permitirá o uso de um protocolo criptográfico, como HTTPS, SFTP ou FTPS, para a transferência segura de Conteúdo do Cliente para e do Serviço Kyndryl por meio de redes públicas.

e. A Kyndryl criptografará o conteúdo inativo se e quando especificado em um Documento de Serviços Kyndryl. Caso um Serviço Kyndryl inclua o gerenciamento de chaves criptográficas, a Kyndryl manterá procedimentos documentados para geração, emissão, distribuição, armazenamento, rotação, revogação, recuperação, backup, destruição, acesso e uso de chaves de segurança.

f. Se a Kyndryl precisar de acesso ao Conteúdo para fornecer os Serviços Kyndryl e tal acesso for gerenciado pela Kyndryl, ele será restrito ao nível mínimo obrigatório. Tal acesso, incluindo o acesso administrativo a qualquer Componente subjacente (acesso privilegiado), será individual, baseado em função e está sujeito à aprovação e validação regular pela equipe autorizada da Kyndryl, de acordo com os princípios de segregação de funções. A Kyndryl manterá medidas para identificar e remover contas redundantes e inativas que tenham acesso privilegiado e revogará prontamente esse acesso mediante o desligamento do proprietário da conta ou mediante solicitação de funcionários autorizados da Kyndryl, como o gerente do proprietário da conta.

g. De acordo com as práticas padrão de mercado e até o limite suportado nativamente por cada Componente, a Kyndryl manterá medidas técnicas para a imposição de tempo limite para sessões inativas, bloqueio de contas após várias tentativas consecutivas de login com falha, autenticação de senha forte ou passphrase, frequência de mudança de senha e ações que possibilitem a transferência e o armazenamento seguros de tais senhas e passphrases.

h. A Kyndryl monitorará o uso de acesso privilegiado e manterá informações de segurança e medidas de gerenciamento de eventos destinadas a: (1) identificar atividade e acesso não autorizados, (2) facilitar o fornecimento de respostas rápidas e adequadas e (3) permitir a execução de auditorias internas e independentes de terceiros quanto à conformidade com a política documentada da Kyndryl.

i. Os logs nos quais o acesso e a atividade privilegiados são registrados serão mantidos em conformidade com a política da Kyndryl. A Kyndryl manterá medidas projetadas para proteção contra o acesso não autorizado, a modificação e a destruição acidental ou deliberada desses registros.

j. Na medida do suportado pelo dispositivo nativo ou pela funcionalidade do sistema operacional, a Kyndryl manterá proteções de computação para seus sistemas de usuário final, que incluem, mas não se limitam a, firewalls de terminal, criptografia completa de disco, detecção e remoção de malware, bloqueios de tela baseados em tempo, e soluções de gerenciamento de terminal que impõem requisitos de correção e configuração de segurança.

k. A Kyndryl higienizará com segurança qualquer mídia física destinada à reutilização e destruirá quaisquer mídias físicas não destinadas à reutilização, de acordo com as diretrizes do NIST quanto à limpeza de mídias.

9. Integridade de Serviço e Controle de Disponibilidade

a. A Kyndryl: (1) executará avaliações de risco de segurança e privacidade dos Serviços Kyndryl pelo menos uma vez ao ano, (2) executará testes de segurança e avaliações de vulnerabilidades dos Serviços Kyndryl antes da liberação para produção e, depois disso, pelo menos anualmente, (3) executará testes de invasão pelo menos uma vez ao ano, (4) executará varreduras automatizadas de vulnerabilidades dos Componentes subjacentes dos Serviços Kyndryl em relação às melhores práticas de configuração de segurança do mercado, (5) corrigirá as vulnerabilidades identificadas a partir dos testes e varreduras de segurança, com base nas avaliações de risco, exploração e impacto associados, e (6) executará ações adequadas para evitar a interrupção dos Serviços Kyndryl ao executar suas atividades de teste, avaliação, varredura e correção.

b. A Kyndryl manterá medidas destinadas a avaliar, testar e aplicar correções de segurança temporárias recomendadas aos Serviços Kyndryl e sistemas, redes, aplicativos e Componentes subjacentes associados, dentro do escopo dos Serviços Kyndryl. Mediante a determinação de que uma correção de segurança temporária recomendada é aplicável e adequada, esta será implementada pela Kyndryl, de acordo com as diretrizes de severidade e avaliação de risco documentadas, com base nas pontuações das correções no Sistema Comum de Pontuação de Vulnerabilidades, quando aplicável. A implementação de patches recomendados de segurança estará sujeita à política de gerenciamento de mudança da Kyndryl.

c. A Kyndryl manterá políticas e procedimentos visando gerenciar os riscos associados à aplicação de mudanças em seus Serviços. Antes da implementação, as mudanças feitas em um Serviço Kyndryl, incluindo seus sistemas, redes e Componentes subjacentes, serão documentadas em uma solicitação de mudança registrada, que inclua uma descrição, o motivo da mudança, os detalhes e o cronograma de implementação, uma declaração de risco que aborde o impacto sobre o Serviço Kyndryl e seus clientes, o resultado esperado, o plano de recuperação e a aprovação documentada por uma equipe autorizada.

d. A Kyndryl manterá um inventário de todos os ativos de tecnologia da informação utilizados na operação de seus Serviços. A Kyndryl monitorará e gerenciará o funcionamento, incluindo a capacidade, e a disponibilidade dos Serviços Kyndryl e seus Componentes subjacentes.

e. Cada Serviço Kyndryl será avaliado separadamente quanto à continuidade de negócios e aos requisitos de recuperação de desastres, por meio de análises de impacto comercial e avaliações de risco adequadas, para identificar e priorizar as funções de negócios críticas. Cada Serviço Kyndryl terá, até o limite garantido por tais avaliações de risco, planos de recuperação de desastre e de continuidade de negócios validados anualmente, mantidos, documentados e definidos separadamente, e consistentes com as práticas padrão de mercado. Os objetivos de tempo e de ponto de recuperação de um Serviço Kyndryl, se fornecidos no Documento de Serviços Kyndryl relevante, serão estabelecidos considerando a arquitetura e o uso desejado para tal Serviço Kyndryl. A mídia física destinada ao armazenamento externo, se houver, como as mídias contendo arquivos de backup, será criptografada antes do transporte.